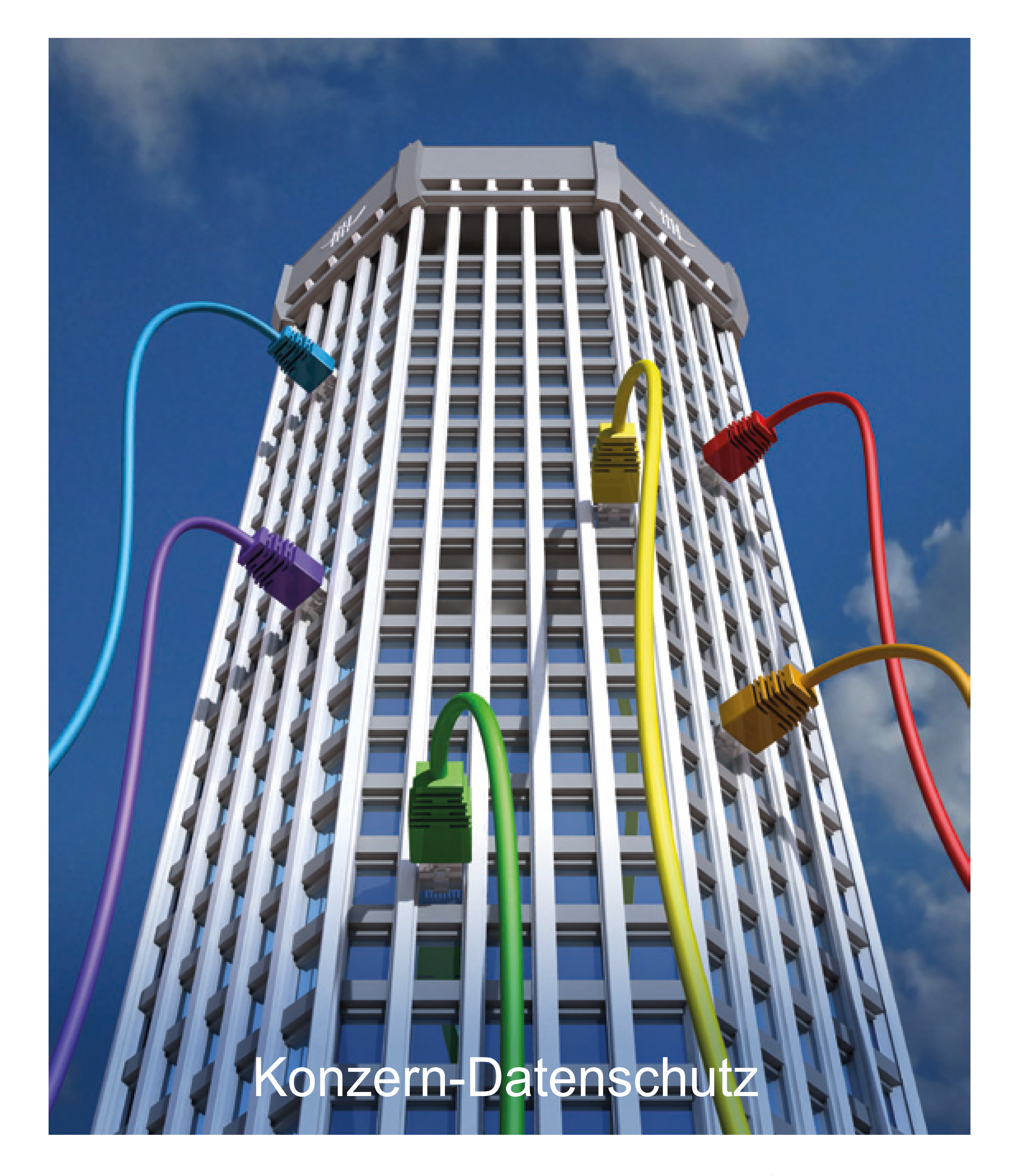
1/2014

Datenschutz Nachrichten

37. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Datenschutz im Konzern ■ Verbraucher wollen Sicherheit und Selbstbestimmung im Netz ■ Datenschutz und Werbung ■ Amtswechsel beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ■ Auszüge aus dem Koalitionsvertrag ■ Russia 1984 ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Montag, 31. März 2014, 18:00 Uhr
EU-Datenschutzreform
Informations- und Disdussionsveranstaltung
Europäische Akademie für Informationsfreiheit
und Datenschutz
Bismarckallee 46/48, 14193 Berlin

Freitag, 11. April 2014, 18:00 Uhr
BigBrotherAwards
Verleihung der Negativ-Preise für Datenkraken
Bielefeld, Hechelei

Samstag, 12. April 2014, 09:30 Uhr
DVD-Vorstandssitzung
Bielefeld. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Donnerstag, 01. Mai 2014
Redaktionsschluss DANA 2/2014
Thema: Internet der Dinge
Verantwortlich: Frank Spaeing

Dienstag, 27. Mai 2014, 09:00 Uhr
Fachtagung Datenschutz in der Medizin
Update 2014
Maritim Hotel München
Goethestraße 7, 80336 München

23. Juni 2014, 09:00 Uhr - 24. Juni 2014, 17:00 Uhr
DuD 2014 - Fachkonferenz
Datenschutz & Datensicherheit
16. COMPUTAS-Jahresfachkonferenz
Leonardo Royal Hotel Berlin

Sonntag, 06. Juli 2014, 10:00 Uhr
DVD-Vorstandssitzung
Berlin. Anmeldung in Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 01. August 2014
Redaktionsschluss DANA 3/2014
Thema: Datenschutz an Flughäfen
Verantwortlich: Frans Valenta

Samstag, 18. Oktober 2014, 16:00 Uhr
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
37. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Karin Schuler
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, soweit nicht anders gekennzeichnet

Editorial

Liebe Leserinnen und Leser,

trotz großer Anstrengung scheitert gerade der Versuch, eine europäische Datenschutzverordnung noch vor den Wahlen zum Europäischen Parlament zu verabschieden. Dies kann man bedauern oder begrüßen, es ist zu befürchten, dass die durch den zuständigen LIBE-Ausschuss verabschiedete Fassung so auch später nicht zur Abstimmung gestellt wird. Der Text hat gegenüber dem ursprünglichen Kommissionsentwurf sehr an Qualität gewonnen. Da er aus Sicht bestimmter Wirtschaftsunternehmen und -branchen jedoch unzumutbare Belastungen enthält, ist daher mit weiterer, grenzwertiger Lobbyarbeit zu rechnen, die der Qualität eines Gesetzes erfahrungsgemäß nicht zuträglich ist.

Mit unserem Schwerpunkt greifen wir ein Thema auf, das Unternehmen, Datenschutzbeauftragten und Arbeitnehmervertretungen seit Jahrzehnten gleichermaßen Kopfschmerzen bereitet. Auch bei den Diskussionen zur geplanten Datenschutzverordnung wurde hierüber sehr kontrovers gestritten. Reinhard Linz gewährt uns Einblick in die Abläufe und Schwierigkeiten bei der Gestaltung von konzernweiten Datenflüssen. Er tut dies aus der Sicht der Arbeitnehmervertretung, stellt dabei aber implizit dar, welche Hausaufgaben ein Unternehmen insgesamt lösen muss. Michaela Zinke betrachtet die Implikationen konzernweiter Datenverarbeitung aus Sicht von Verbrauchern und stellt Forderungen bezüglich der europäischen Regulierung auf. Christoph Schäfer beleuchtet ergänzend –und schön spitzzüngig– auf welche Weise die Aufsichtsbehörden Verbraucher im Haifischbecken der Werbeindustrie zu schützen gedenken.

Anlässlich des Amtswechsels beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit stellt Hans-Hermann Schild Überlegungen zu den Besetzungsmodalitäten an und wir dokumentieren die Rede von Innenminister de Maizière anlässlich der mit dem Amtswechsel verbundenen Feier.

Schließlich dokumentieren wir, neben den üblichen Datenschutznachrichten aus Deutschland und aller Welt, die Passagen des Koalitionsvertrages, in denen die Weichen für datenschutzrelevante Fragen gestellt wurden.

Karin Schuler

Autorinnen und Autoren dieser Ausgabe:

Reinhard Linz
Berater für betrieblichen Datenschutz bei der FORBIT GmbH. linz@forbit.de

Christoph Schäfer
Security Consultant mit dem Beratungsschwerpunkt Datenschutz bei der Secorvo Security Consulting GmbH, Karlsruhe. christoph.schaefer@secorvo.de

Hans-Hermann Schild
Vorsitzender Richter am Verwaltungsgericht Wiesbaden, befasst sich seit fast dreißig Jahren vielseitig mit Themen aus dem Bereich des Rechts auf informationelle Selbstbestimmung und des Datenschutzrechts. Erreichbar über die DVD-Geschäftsstelle.

Michaela Zinke
Referentin im Projekt Verbraucherrechte in der digitalen Welt beim Verbraucherzentrale Bundesverband, Schwerpunkt ihrer Tätigkeit liegt auf den Verhandlungen der EU-Datenschutzgrundverordnung, aber auch die juristische Betrachtung datenschutzrechtlicher Probleme von Internetdiensten, michaela.zinke@vzbv.de, Twitter @Prinze484

Reinhard Linz

Datenschutz im Konzern – Eine Lagebeschreibung aus Betriebsratssicht

„Datenschutz durch Mitbestimmung“ ist eine gängige und durchaus treffende Floskel, wenn Autoren über den Datenschutz im Arbeitsverhältnis schreiben. Natürlich gibt es Datenschutz im Betrieb auch ohne Mitbestimmung. Das Bundesdatenschutzgesetz (BDSG) und die aus dem Grundgesetz abzuleitenden Datenschutzrechte gelten schließlich auch im Arbeitsverhältnis und auch dann, wenn gar kein Betriebsrat gebildet wurde. Aber der Einfluss des Betriebsrats auf den Arbeitnehmerdatenschutz kann sehr groß und sehr nützlich sein. Wir werfen einen Blick darauf, in welcher Weise die besonderen Rahmenbedingungen in einem Konzern die Einflussmöglichkeiten des Betriebsrats prägen.

Starke Rechte für den Betriebsrat

Praktisch die gesamte Verarbeitung von Arbeitnehmerdaten im Betrieb unterliegt nach dem Betriebsverfassungsgesetz (BetrVG) den Beteiligungsrechten der Betriebsräte, in weiten Bereichen sogar harten Mitbestimmungsrechten. Dreh- und Angelpunkt ist das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 über technische Einrichtungen, die zur Leistungs- oder Verhaltenskontrolle geeignet sind. Damit sind so gut wie alle computergestützten Systeme erfasst. Hinzu kommen das Informations- und Beratungsrecht über die Planung von technischen Anlagen (§ 90), die Mitbestimmung über Personalfragebögen (§ 94) und über die Ordnung und das Verhalten der Arbeitnehmer im Betrieb (§ 87 Abs. 1 Nr. 1), der Auftrag nach § 75 Abs. 2, die freie Entfaltung der Persönlichkeit der Arbeitnehmer zu schützen und zu fördern, sowie der Auftrag nach § 80 Abs. 1 Nr. 1 über die Einhaltung zugunsten der Arbeitnehmer geltender Rechtsvorschriften zu wachen. Ob Arbeitszeiterfassung, Produktionsplanung, Mitarbeiterbefragungen, Personalinformationssysteme oder Social Media im Unternehmen, der Betriebsrat ist zu beteiligen.

Natürlich ist in allen genannten Beispielen auch der betriebliche Datenschutzbeauftragte im Spiel. Aber der Betriebsrat ist mächtiger. Er ist bei der Gestaltung der betrieblichen Datenverarbeitungsprozesse nicht nur Beratungspartner des Managements. In den meisten Fällen ist seine explizite Zustimmung erforderlich, bevor ein System in Betrieb gehen darf. Und während Betriebsräte bei Verletzung dieses Rechts immer wieder die Arbeitsgerichte anrufen, hört man nur selten, dass ein Datenschutzbeauftragter die Aufsichtsbehörde zu Hilfe ruft, wenn sein Rat zur DV-Gestaltung unbeachtet bleibt.

Verstärkung für den Datenschutz

Nützlich ist der Einfluss der Betriebsräte, weil sie Regelungen für die Datenverarbeitung herbeiführen, die die spezifischen Gegebenheiten eines bestimmten Geschäftsprozesses in ihrem individuellen Unternehmen berücksichtigen und daher praxisnäher und viel konkreter sein können, als die stets generell-abstrakten Gesetzesvorschriften. Während das Gesetz recht allgemein verlangt, dass nur die personenbezogenen Daten gespeichert werden dürfen, die für einen legitimen Zweck erforderlich sind, kann eine Betriebsvereinbarung (BV) eine genaue Auflistung der Datenarten enthalten, die z.B. in einer Rückmeldung aus der Auftragsfertigung von Motoren am Unternehmensstandort Köln erfasst werden sollen.

Betriebsräte können auch System-Revisionen durchführen und gegen Verletzungen von IT-Betriebsvereinbarungen notfalls gerichtlich vorgehen. Die politischen Handlungsoptionen kommen noch dazu. Wenn ein Betriebsrat den Arbeitnehmerdatenschutz konsequent verfolgt, in Betriebsversammlungen und Publikationen immer wieder thematisiert, für Schulung und Aufklärung sorgt, dann hat das erheblichen Einfluss darauf, welchen Stellenwert dem Datenschutz in der gesamten Betriebskultur zugemessen wird.

So bietet sich für Betriebsräte ein weites Feld, um sozusagen als Lobbyisten für die Betroffenen, hier die Arbeitnehmer, tätig zu werden. Die Möglichkeiten zu nutzen und den eigenen Zielen gerecht zu werden, ist allerdings schon in einem einzelnen Betrieb nicht leicht. In einem Konzern wird es noch ein Stück schwieriger.

Große Konzerne – Große Systeme – Große Aufgaben für kleine Gremien

Wenn Konzernunternehmen ihre Geschäftsprozesse standardisieren und miteinander verzahnen, verzahnen sie selbstverständlich auch ihre Datenverarbeitung in gemeinsam genutzten IT-Systemen. Und die sind typischerweise groß. Hierbei geht es nicht um Kantinenabrechnung oder Parkplatzverwaltung, wobei Daten von Beschäftigten eines einzelnen Standorts verarbeitet werden. Vielmehr geht es um Systeme von Anbietern wie SAP, SuccessFactors oder Taleo, die das zentrale Personalmanagement unterstützen sollen und für den ganzen Konzern sämtliche Stellenausschreibungen, die Bewerberauswahl, die Dokumentation von Zielvereinbarungen, die Beurteilung von Beschäftigten, die Verteilung von Gehältern und Prämien, die Suche nach passenden Mitarbeitern für freie Stellen, die Karriere- und Nachfolgeplanung und die Personalentwicklungspläne und -maßnahmen abbilden. Ähnliche Großsysteme gibt es

für das zentrale Controlling, die Produktionsplanung, die Lagerverwaltung, die Kundenbetreuung und vieles mehr.

Um allein die technischen Funktionen solcher Systeme zu verstehen, Risiken zu identifizieren und Gestaltungsoptionen zu erkennen, brauchen selbst „technik-affine" Menschen sehr viel Zeit und Bereitschaft, sich in die Besonderheiten eines Systems einzuarbeiten. Die arbeitsorganisatorische Seite kommt noch dazu. Es gilt, die von der Integration betroffenen Geschäftsprozesse an den einzelnen Standorten zu betrachten, da sie einerseits ein wichtiges Maß für die Erforderlichkeit der personenbezogenen Datenverarbeitung darstellen, andererseits aber auch selbst nach Datenschutzkriterien (um-)gestaltet werden müssen. Dabei werden Betriebsräte ein besonderes Augenmerk auf die Bedürfnisse der Arbeitnehmer nach Erhalt und Qualität der Arbeit sowie auf deren Gewohnheiten und Präferenzen haben, auf Aspekte also, die zusätzlich zu den klassischen Arbeitgeberzielen Effektivität und Effizienz mit dem Datenschutz in Einklang gebracht werden sollen. Hier entsteht für die Betriebsräte ein Kapazitätsproblem. Für Konzernbetriebsräte (KBR) kann das in besonderem Maße zutreffen; denn anders als bei den örtlichen Betriebsräten wächst die Zahl ihrer Mitglieder im Allgemeinen nicht parallel zur Zahl der vertretenen Beschäftigten.

So fällt die Aufgabe, für eine sehr große Zahl von Beschäftigten an verschiedenen Standorten den Arbeitnehmerdatenschutz in vielfach verästelten Geschäftsprozessen zu gestalten, oftmals einer sehr kleinen Zahl von Konzernbetriebsratsmitgliedern zu, für die der Arbeitnehmerdatenschutz obendrein nur eine von vielen Aufgaben darstellt.

Datenschutz-Controlling

Mehr Arbeitskraft und mehr Kompetenz sind die naheliegenden Forderungen angesichts dieser Schwierigkeiten. Tatsächlich konnten manche Betriebsräte durch Vereinbarungen über die Größe der Gremien oder die Zahl der Freistellungen eine gewisse Entlastung schaffen.

Unabhängig davon können Betriebsräte nach § 80 Abs. 2 BetrVG die Unterstützung „sachkundiger Arbeitnehmer" in Anspruch nehmen, die sich bei den Arbeitsabläufen oder in der Technik auskennen und nicht selbst Mitglied des Gremiums zu sein brauchen. Selbstverständlich kann auch der betriebliche Datenschutzbeauftragte mit seiner Sachkunde helfen. Wenn geeignete interne Experten fehlen oder der Betriebsrat an deren Unbefangenheit zweifelt, kann er nach § 80 Abs. 3 BetrVG auch externe Sachverständige seines Vertrauens zu Rate ziehen.

Leider zeigt die Erfahrung, dass all dies das Kapazitäts- und Kompetenzproblem lindert, aber nicht strukturell löst. Einem erweiterten Projektteam auf der Betriebsratsseite gelingt dann vielleicht nach monatelanger Arbeit eine ordentliche Regelung zum Datenschutz in *einem* System. Währenddessen aber werden durch die Einführung oder Änderung anderer Systeme Fakten geschaffen, die der Betriebsrat – und oft auch der nicht minder überlastete Datenschutzbeauftragte – erschöpft hinnehmen, ohne sie wesentlich beeinflusst oder auch nur gründlich geprüft zu haben.

Aussichtsreicher wäre es, dem strukturellen Mangel strukturell zu begegnen, indem man verbindliche Standards für DV-Projekte schafft. So wie ein Kostencontrolling heute selbstverständlich zur Projektarbeit gehört, sollte auch eine Art Datenschutz-Controlling eine Standard-Aufgabe jedes DV-Projekts sein. Konformität mit geltenden Datenschutzvorschriften, besser noch Datenschutz-Exzellenz sollte zum unverzichtbaren Qualitätsmerkmal jedes DV-Prozesses erklärt werden, und die dafür notwendigen Arbeiten sollten *in* den Projekten geleistet werden. Die Projektleitung ist dann nicht nur dafür verantwortlich, dass nach dem Projekt ein neues DV-Verfahren funktioniert, sondern auch dafür, dass alle Datenschutzanforderungen erfüllt sind.

Die Datenschutzaufgaben gehören selbstverständlich in den Projektplan. Wie bei jeder anderen Projektaufgabe sind die erwarteten Ergebnisse zu definieren, die ausführenden Personen sind zu benennen, der erwartete Zeitbedarf und die Kosten sind zu planen, und – sehr wichtig – die Meilensteine sind so zu fixieren, dass auch Datenschutzergebnisse geprüft und freigegeben werden. Betriebsrat und Datenschutzbeauftragter gehören dann zu den Freigabe-Instanzen sowohl für den Projektplan als auch für das Passieren der Meilensteine. Die Erarbeitung der notwendigen Datenschutzergebnisse kann man ihnen jedoch nicht, jedenfalls nicht vollständig aufbürden. Das wird bei der Kapazitätsplanung des Projektes schnell deutlich werden.

Zu den Pflichtaufgaben jedes DV-Projektes muss es gehören, mindestens die folgenden, für den Datenschutz wichtigen Konzepte zu erarbeiten und zu dokumentieren:

- Datenmodell: Welche personenbezogenen Daten werden zu welchem Zweck verarbeitet, und worin begründet sich die Erforderlichkeit?
- Löschkonzept: Welche Daten müssen wann gelöscht werden, und mit welchen organisatorischen und technischen Verfahren geschieht das?
- Auswertungskonzept: Wie und zu welchem Zweck werden personenbezogene Daten ausgewertet und wodurch ist die Erforderlichkeit begründet?
- Betriebliches Berechtigungskonzept: Welche Stellen müssen welche Informationen bekommen?
- Technisches Berechtigungskonzept: Wie werden Zugriffsbeschränkungen technisch realisiert?
- Konzept für die Datenweitergabe: Wer ist Empfänger der personenbezogenen Daten, welche Rechtsgrundlage erlaubt die Datenweitergabe und welche Verträge werden mit den Datenempfängern als Dritte im Sinne des BDSG oder als Auftragsdatenverarbeiter abgeschlossen?
- Revisionskonzept: Welche technischen und organisatorischen Hilfsmittel stehen für die Datenschutz-Revision zur Verfügung?
- Sicherheitskonzept: Mit welchen Maßnahmen wird den im vorliegenden Fall zu beachtenden Sicherheitsanforderungen Rechnung getragen?

Diese Themen überschneiden sich mit den Themen des Verfahrensverzeichnisses nach §§ 4e und 4g BDSG. Die Angaben sollten aber detaillierter ausfallen, als es in den Verfahrensverzeichnissen üblich ist. Für viele der notwendigen Datenschutz-Dokumente kann man Fragenraster, Checklisten oder gar Formulare vorbereiten, was den gewünschten

Detaillierungsgrad festlegt, eine gewisse Mindestqualität sichert und insgesamt die Arbeit erleichtert.

Der Konzernbetriebsrat könnte sich bemühen, ein solches Datenschutz-Pflichtprogramm für jedes DV-Projekt in eine IT-Rahmenbetriebsvereinbarung aufzunehmen. Das wäre zwar eine freiwillige, nicht per Einigungsstelle erzwingbare Vereinbarung, würde also die grundsätzliche Bereitschaft des Managements voraussetzen, sich auf derartige Standards einzulassen. Man würde damit aber jenseits schöner Worte in Broschüren und auf Homepages den Datenschutz wirklich zum festen Bestandteil der Geschäftsprozesse machen. Betriebsräte und Datenschutzbeauftragte würden entlastet, weil sie Datenschutzkonzepte mehr beurteilen als entwickeln müssten, und praxisnahe Datenschutz-Vorkehrungen würden in jeden Verarbeitungsprozess sozusagen von vornherein eingebaut. Und – was im Zeitalter der Kennzahlen-Fixierung nicht zu unterschätzen ist – ein erheblicher Teil der Kosten für die Datenschutzarbeiten würde verursachungsgerecht den DV-Projekten zugeordnet und nicht, wie es sonst oft geschieht, dem Betriebsrat oder dem Datenschutzbeauftragten.

Diffuser Informationsbedarf in der Matrixorganisation

Modern und typisch für große Unternehmen und Konzerne ist die sogenannte Matrix-Organisation: Beschäftigte werden nach verschiedenen Ordnungskriterien in mehrere Hierarchien eingebunden und haben in der Folge nicht mehr nur einen Chef, sondern gleich mehrere direkte Vorgesetzte. Der herkömmliche Chef wird zum sogenannten „disziplinarischen Vorgesetzten“. Daneben gibt es aber „funktionale Vorgesetzte“, z.B. einen in der Spartenhierarchie Nutzfahrzeuge, einen in der Funktionshierarchie Konstruktion und schließlich noch den Leiter eines einzelnen Projektes Elektrocaddy Zürich. Eine solche Struktur lässt sich gar nicht mehr in den zwei Dimensionen einer Matrix darstellen. Daher trägt man in das klassische Organigramm neben der Baum-Hierarchie, die die disziplinarische Ordnung repräsentiert, noch gestrichelte Linien („Dotted Lines“) ein, die die anderen Hierarchien darstellen sollen. Es entsteht ein Bild, das eher einem Gestrüpp als einer Ordnung gleicht. Wenn zusätzlich – und das ist in Konzernen durchaus normal – abgesehen von der disziplinarischen alle Vorgesetztenhierarchien kreuz und quer durch die Konzernunternehmen verlaufen, ist das Organigramm endgültig nicht mehr grafisch darstellbar.

Klar ist, dass jeder der verschiedenen Vorgesetzten irgendwelche Informationen über die ihm zugeordneten Beschäftigten braucht, seien es Urlaubszeiten, Qualifikationen, Bezüge, Interessen, vereinbarte Ziele oder Beurteilungen. Was genau welcher Vorgesetzte wissen muss, ist aber kaum zu ermitteln; denn die Aufgaben und Kompetenzen in der komplizierten Struktur sind oftmals gar nicht oder nur sehr vage definiert. Obendrein ändert sich diese Struktur in großen Unternehmen tatsächlich jeden zweiten Tag, und es gibt keine Stelle und keine Dokumentation, die über den aktuellen Stand verlässlich Auskunft geben könnten.

Auf der Grundlage solcher Strukturen, die erforderlichen und damit legitimierbaren Datentransfers bzw. Zugriffsberechtigungen in IT-Systemen zu ermitteln, ist – gelinde gesagt – eine Herausforderung für die Datenschützer. Der Sog zu einer Totalfreigabe aller Mitarbeiterdaten für alle Vorgesetzten („damit nur alle ihren Job erledigen können“) ist enorm, aber sicher nicht angemessen.

Worauf der Betriebsrat und ebenso der Datenschutzbeauftragte hier drängen sollten, ist

- klare Aufgabendefinition und Aufgabentrennung in der multidimensionalen Hierarchie,
- Beweislast für die Erforderlichkeit eines Datenzugriffs bei den Antragstellern und
- notfalls auch eine durch den Datenschutz begründete Änderung der Organisationsstruktur hin zu klar abgegrenzten, reduzierten Zuständigkeiten.

Insofern kann die Mitbestimmung des Betriebsrats über den Arbeitnehmerdatenschutz indirekt zu einer – begrenzten – Mitbestimmung über die Arbeitsorganisation werden, obwohl die an sich nicht der Mitbestimmung unterliegt. Solches durchzusetzen, ist zwar bestimmt nicht einfach, ist aber begründet durch die Notwendigkeit, die Anwendung technischer Überwachungseinrichtungen auch organisatorisch zu gestalten.

Datenaustausch über Unternehmensgrenzen hinweg – Betriebsvereinbarungen als Rechtsgrundlage

Konzerne organisieren ihre Arbeit über Unternehmensgrenzen hinweg. Produktionssegmente und auch Managementfunktionen werden auf wenige Standorte konzentriert. Konzerninterne Fertigungsketten, die sich über verschiedene Standorte erstrecken, werden eng aufeinander abgestimmt. Für manche Verwaltungsfunktionen werden sogar neue Konzernunternehmen gegründet, sogenannte Shared-Service-Organisationen, die dann sozusagen als gemeinsame Fachabteilungen für mehrere Konzernunternehmen Standard-Dienste wie zum Beispiel den Einkauf, das Finanz-Controlling oder die Personalverwaltung übernehmen. Aber auch strategische Management-Funktionen werden in sog. Centers of Expertise gebündelt und einem einzigen federführenden Unternehmen für eine ganze Region wie etwa Europa, den mittleren Osten und Asien („EMEA“) zugeordnet. Im Personalbereich werden dann z.B. die Konzeption und die Umsetzung einheitlicher Entlohnungssysteme, Personalbeurteilungsverfahren, Karrierewege und Stellenbesetzungsverfahren von einem CoE HR zentral beobachtet und gesteuert.

Diese Organisationsformen – meist gekoppelt mit multidimensionalen Matrix-Strukturen – verursachen Datenströme zwischen Unternehmen, die einer besonderen Rechtsgrundlage bedürfen und, weil gesetzliche oder tarifvertragliche Regelungen hierzu höchstens ausgestaltungsbedürftige Rahmenregeln vorgeben, zugleich Gegenstand der Mitbestimmung sind.

Sofern die Datenübertragung im Rahmen einer Auftragsdatenverarbeitung innerhalb Europas erfolgt, bildet § 11 BDSG die Erlaubnisnorm. Allerdings dürfte die Arbeitsverteilung im Konzern die Merkmale einer Auftragsdatenverarbeitung nur in Ausnahmefällen erfüllen, etwa beim reinen Rechenzentrumsbetrieb durch eine Konzerntochter. Selbst Shared-Service-Organisationen,

die überwiegend Standard-Dienstleistungen erbringen, haben oft so große Freiräume bei der Erledigung ihrer Aufgaben, dass man von einer Funktionsübertragung ausgehen muss. Wenn eine Shared-Service-Organisation für das Beschäftigungsverhältnis erforderliche Dienstleitungen erbringt, z.B. das Reisemanagement oder die Entwicklung individueller Schulungspläne für Konzernmitarbeiter, kann damit auch eine im Sinne von § 32 BDSG erforderliche Datenübermittlung für Zwecke des Beschäftigungsverhältnisses verbunden sein. Soweit jedoch Daten für das strategische Management, für die Koordination verteilter Produktionsprozesse oder eine konzernweite Personalvermittlung übertragen werden, kommt eine Auftragsdatenverarbeitung nicht in Betracht, weil die Daten von den Empfängern auch für eigene Zwecke genutzt werden, und § 32 greift nicht, weil dies Zwecke sind, die außerhalb des individuellen Beschäftigungsverhältnisses liegen.

Dann kann es mit der datenschutzrechtlichen Erlaubnisnorm schwierig werden, erst recht natürlich, wenn sensible Arbeitnehmerdaten wie zum Beispiel Qualifikationen und Beurteilungen oder krankheitsbedingte Fehlzeiten kommuniziert werden sollen. Meistens läuft es auf die Frage hinaus, ob die Abwägung der Interessen der verantwortlichen Stelle mit denen der Betroffenen gemäß § 28 Abs. 1 Ziff. 2 BDSG zu Gunsten des Unternehmens ausfällt, das die Daten an seine Konzernschwestern weitergeben will. Bei dieser Abwägung ist die Gesamtsituation zu würdigen, in der der Datentransfer stattfinden soll, und die wird auch von geltenden Betriebsvereinbarungen geprägt. Je besser die betroffenen Arbeitnehmer trotz Übermittlung ihrer Daten im Konzern vor Verletzungen ihres Persönlichkeitsrechts geschützt werden, desto geringer ist in diesem Abwägungsprozess ihr Interesse am Ausschluss der Übermittlung zu werten. Sollte also eine Konzernbetriebsvereinbarung insgesamt enge Grenzen für die Verarbeitung und Nutzung der im Konzern kommunizierten Arbeitnehmerdaten ziehen, indem sie z.B. Verwendungszwecke, Zugriffsberechtigungen, Löschfristen und Revisionsverfahren für alle beteiligten Konzernunternehmen festlegt, könnte dies den Ausschlag dafür geben, dass die Datenübermittlung zulässig ist. Wenn die Konzernunternehmen nicht durch andere Verträge vergleichbare Verpflichtungen eingegangen wären, hätten KBR und Konzernleitung damit als Ergebnis der Mitbestimmung überhaupt erst eine datenschutzrechtliche Zulässigkeitsvoraussetzung geschaffen, die sonst gefehlt hätte.

Wenn die Datenübermittlung nicht nur Unternehmens-, sondern auch Ländergrenzen überschreitet, sind die Empfänger nicht dem BetrVG unterworfen. Dann kann eine Betriebsvereinbarung ihre legitimierende Wirkung nur in Kombination mit einem Vertrag zwischen den Konzernunternehmen entfalten, der die ausländischen Töchter zur Einhaltung der dort festgelegten Regeln verpflichtet. Die besonderen Voraussetzungen nach den §§ 4b und 4c BDSG für eine Datenübermittlung ins Ausland, namentlich in Länder außerhalb von EU und EWR müssen natürlich zusätzlich erfüllt sein.

Eine Betriebsvereinbarung kommt allerdings auch als eigenständige Rechtsgrundlage in Betracht, wenn sie die Datenübermittlung als „andere Rechtsvorschrift" im Sinne von § 4 Abs. 1 BDSG erlaubt. Eine knappe Betriebsvereinbarung, in der ein großzügiger Betriebsrat der Übermittlung von Arbeitnehmerdaten vorbehaltlos zustimmt, würde allerdings noch nicht ausreichen, weil die aus den Grundrechten ableitbaren Mindeststandards des Persönlichkeitsschutzes sichergestellt sein müssen. Es ist jedoch keineswegs geklärt, in welche ergänzenden Vorschriften die Übermittlungserlaubnis einer BV eingebettet sein muss, um die Standards der Verfassung zu erfüllen. Sie dürften den bei der Interessenabwägung abzulegenden Maßstäben ähnlich sein.

Ob als Faktor bei der Interessenabwägung oder als „andere Rechtsvorschrift" – klar ist, dass eine Betriebsvereinbarung eine datenschutzrechtliche Grundlage schaffen kann, die die Datenübermittlung im Konzern erst zulässig macht. Entsprechend sorgsam sollten die Betriebsparteien vorgehen, damit der durch das BDSG gewährte Schutz der Daten nicht aufgeweicht, sondern möglichst gestärkt wird.

Falsche Verhandlungspartner

In ausländisch geführten Konzernen ergeben sich für den Betriebsrat bei seinen Bemühungen um den Datenschutz oft besondere Schwierigkeiten.

Ein verbreitetes Problem besteht darin, dass dem Betriebsrat ein kompetenter Verhandlungspartner fehlt. Häufig sitzt er Managern einer deutschen Konzerntochter gegenüber, die wichtige Entscheidungen gar nicht selbst treffen dürfen, sondern sich erst bei „höheren" Stellen im Ausland rückversichern müssen. Wenn auch noch das für die IT federführende Unternehmen seinen Sitz im Ausland hat, sind manche deutsche Geschäftsführer nicht einmal imstande, über die Datenverarbeitungsprozesse und die Einrichtung der beteiligten IT-Systeme fundiert Auskunft zu erteilen.

Diese Situation macht die Beratungen außerordentlich zäh und mühsam. Die Kommunikation mit den Fachleuten im Hintergrund verläuft schleppend und mit vielen Missverständnissen. Denn in Paris, San Diego und Bangalore hat man nur vage Vorstellungen davon, was ein Betriebsrat ist, warum er so viele Fragen zu Sonderaspekten der Datenverarbeitung stellt und was das mit den Interessen von Beschäftigten zu tun hat. Auch die grundlegenden Vorstellungen von Datenschutz und seiner Bedeutung erweisen sich als unterschiedlich. So erhält man Auskünfte, die formal korrekt sein mögen, aber die falschen Schwerpunkte setzen und nicht wirklich weiterhelfen. Zusagen, bestimmte Daten nicht zu speichern, auf manche Auswertungen zu verzichten oder Berechtigungen einzuschränken, sind noch schwerer zu bekommen. Warum sollte man sich hier festlegen? Bloß weil ein Betriebsrat in Deutschland das will?

Um voranzukommen und am Ende ein gutes Ergebnis zu erzielen, müssen Fachleute und Entscheider an den Verhandlungstisch. Sind die in Deutschland nicht anzutreffen, sollten auch Auslandsreisen kein Hindernis sein. Wenn der europäische IT-Chef gemeinsam mit seinem SAP-Berechtigungsexperten aus Helsinki nach Köln fliegt, um mit dem Gesamtbetriebsrat zu verhandeln, sind beide formal nicht die Repräsentanten des der Mitbestimmung unterliegenden Unternehmens. Trotzdem führen derarti-

ge Gespräche erfahrungsgemäß schneller zum Ziel: Neben dem Austausch über Interessen und Absichten kann man zügig zu den Kernfragen kommen und die Gestaltungsoptionen klären. Nur wenn sich verhandlungsfähige Personen gegenübersitzen, kommt Bewegung in die Sache: Positionen können überdacht und Kompromisslinien ausgelotet werden. So wird mancher Knoten durchschlagen, der im schriftlichen „Antragsverfahren" nur immer dicker geworden wäre. Nach dem zweiten Treffen können dann auch Videokonferenzen fruchtbar verlaufen. Damit Datenschutz gelingt, müssen die richtigen Leute einander kennenlernen. In internationalen Konzernen kann das internationale Verhandlungskommissionen erforderlich machen.

Internationale Umzingelung

Ein weiteres Problem ist spiegelbildlich zum ersten: Auch der ausländischen Konzernmutter fehlt ein Gegenpart, mit dem sie über den Arbeitnehmerdatenschutz im Konzern verhandeln könnte oder müsste. Es gibt keinen „globalen" Betriebsrat, der alle Arbeitnehmer eines Konzerns vertritt. Die gemeinsame Vertretung der in der EU beschäftigten Arbeitnehmer eines Konzerns ist der Europäische Betriebsrat; er hat jedoch nur Informations- und Beratungsrechte. Innerhalb und erst recht außerhalb der EU gibt es kaum ein Land, in dem die Arbeitnehmervertretung in Sachen Datenverarbeitung ähnlich harte Mitbestimmungsrechte hat wie in Deutschland.

So können amerikanische und asiatische Konzerne internationale Informationssysteme weitgehend ohne Mitbestimmung durch Arbeitnehmervertretungen aufbauen. Und das ist der bevorzugte Weg: Das Kernsystem wird in Japan eingerichtet und in Betrieb genommen und dann nach und nach in den Tochtergesellschaften in anderen Ländern „ausgerollt" z.B. in der Reihenfolge Korea, Kanada, Südafrika, England, Frankreich, Skandinavien, Benelux und Polen bis am Ende Deutschland und vielleicht Österreich regelrecht umzingelt sind von den Ausläufern des großen, vernetzten Informationssystems.

Nachdem das System seit mehreren Jahren in allen anderen Ländern produktiv eingesetzt wird, tritt der deutsche Betriebsrat in die Verhandlungen über Datenkataloge, Schnittstellen, Leistungskennzahlen und Zugriffsberechtigungen ein, weil das System nun auch in Deutschland eingeführt werden soll. Die verbleibenden Optionen zu seiner Ausgestaltung und Einsatzweise sind jetzt nur noch marginal, die Verhandlungsspielräume der deutschen Manager auch. Ihre persönliche Leistungsbeurteilung und der Jahresbonus hängen davon ab, ob der Anschluss der deutschen Niederlassung bis zum nächsten Jahreswechsel vollzogen ist. Wo kann das hinführen?

Wenn der Betriebsrat auf seinen Gestaltungsanspruch pocht und Forderungen zur Verbesserung des Arbeitnehmerdatenschutzes stellt, werden die Verhandlungen bald scheitern, und die Arbeitgeberseite wird angesichts ihres Termindrucks in die Einigungsstelle streben.

Nun kommt es auf den Vorsitzenden an. Das wird höchstwahrscheinlich ein Arbeitsrichter sein, und er wird zu Beginn der Verhandlungen betonen, dass auch internationale Konzerne in Deutschland deutsches Arbeitsrecht beachten müssen. Aber nach welchen Kriterien wird er die Forderungen des Betriebsrats nach einer (Um-)Gestaltung der vom neuen System geprägten DV-Prozesse bewerten? Wie stark wird er sich von den „immensen Kosten" beeindrucken lassen, die die Arbeitgeberseite für die verlangten Anpassungen vorhersagt? Wird er eine auf konkrete Zahlen gestützte Kostenprognose verlangen? Und welches Gewicht wird er dem Gebot des § 90 BetrVG beimessen, über die Planung technischer Anlagen so rechtzeitig mit dem Betriebsrat zu beraten, dass die „Vorschläge und Bedenken des Betriebsrats bei der Planung berücksichtigt werden können"? Gerade auch um die Einflussmöglichkeiten zu sichern, hat der Betriebsrat außerdem nach § 87 Abs. 1 Nr. 6 BetrVG nicht nur bei der Anwendung, sondern schon bei der Einführung technischer Einrichtungen mit Überwachungspotential ein Mitbestimmungsrecht. Sieht der Vorsitzende das Informations-, Beratungs- und Mitbestimmungsrecht also schon verletzt, und ist das Kostenargument wegen der bisher vorenthaltenen Einflussmöglichkeiten nur noch von geringem Gewicht?

Es bedarf schon eines soliden Selbstbewusstseins des Vorsitzenden, um trotz des massiven Drängens eines Weltkonzerns im Verfahren genügend Zeit für eine verständliche Darstellung der geplanten DV-Verfahren, für eine ernsthafte Erwägung aller Datenschutzaspekte und eine gründliche Analyse der objektiven Gestaltungsoptionen zu reservieren. Denn schon dies kann etliche Sitzungstage in Anspruch nehmen. Dem Unternehmen in einem Spruch dann auch noch kostspielige und erneut zeitraubende Umbauten am System zuzumuten, kommt schon einer Mutprobe gleich, der die meisten Vorsitzenden lieber ausweichen werden.

Es kommt aber auch auf die Entschlossenheit des Betriebsrats an, und die bestimmt sich nicht allein nach der Güte der verhandelten Datenschutzregelungen. Vielmehr spielen noch ganz andere Faktoren eine Rolle, die für die Beschäftigten unter Umständen eine viel handfestere Bedeutung haben. Da geht es zum Beispiel um Arbeitsplätze. Wenn die Geschäftsprozesse nicht rationalisiert und global integriert werden, leidet die Konkurrenzfähigkeit des gesamten Unternehmens. Sogar die konzern-interne Konkurrenz entfaltet ihre Wirkung. Wenn die Datenschutzanforderungen in Köln so kompliziert werden und letztlich die Geschäftsprozesse behindern, dann erhält vielleicht das Werk in Prag den Zuschlag für die neue Produktlinie. Auch wenn nie ganz sicher ist, ob solche Befürchtungen sich bewahrheiten, machen sie es dem Betriebsrat schwer, für die deutschen Standorte als den einzigen im ganzen Konzern eine strikte Haltung beim Arbeitnehmerdatenschutz aufrechtzuerhalten und gegenüber seinen Wählern zu begründen.

Das pragmatische Ergebnis besteht dann oft darin, dass im Wesentlichen der in den Nachbarländern etablierte Ist-Stand als Soll für die deutsche Konzerntochter festgeschrieben wird. Der Betriebsrat kann dann bei künftigen Änderungen erneut mitbestimmen. Das Feld echter Gestaltung aber schrumpft auf das Schulungskonzept für die neuen Benutzer in Deutschland (mit verpflichtender Sensibilisierung für die neuen Datenschutz-Risiken) und auf die Zusicherung eines jederzeitigen Revisionsrechts auch beim ausländischen System-

betreiber und dies vielleicht sogar mit einem dafür einzurichtenden eigenen Systemzugang.

Es zeigt sich deutlich, dass die Gestaltung des Arbeitnehmerdatenschutzes keineswegs nur eine Frage des Rechts ist, sondern in hohem Maße von den Überzeugungen, dem Willen und der Kompetenz der Akteure, letztlich also von Macht und Politik bestimmt wird. Das mag vielleicht erschrecken, ist aber in der betrieblichen Demokratie ganz normal und kann bei Wahrung fairer Umgangsformen auch durchaus gute Früchte tragen. So ist es eben beim „Datenschutz durch Mitbestimmung".

Michaela Zinke

Verbraucher wollen Sicherheit und Selbstbestimmung im Netz

Die Digitalisierung beeinflusst den Alltag der Verbraucher zunehmend. Nur wenige Anbieter dominieren dabei den digitalen Markt. Google besitzt in Deutschland ein faktisches Monopol von 96 Prozent bei den Suchmaschinen und beherrscht den Markt der digitalen Werbung. Amazon ist mit Abstand der führende E-Commerce-Anbieter, mit dem nur wenige deutsche Unternehmen Schritt halten können. Facebook wird hierzulande mittlerweile von rund 23 Millionen Menschen genutzt und hat den ehemaligen deutschen Marktführer bei sozialen Netzwerken, StudiVZ, längst ins Abseits gedrängt. Google, Apple, Facebook und Amazon werden nicht nur am meisten genutzt, sondern vereinen auch einen bedeutenden Teil der Umsätze im Internet auf sich. Diese Quasi-Monopolisten generieren Gewinne durch umfassende Datensammlungen. Entscheidend für sie ist, wie man Nutzerinteraktionen am effektivsten zu Geld machen kann. In der digitalen Welt sind Verbraucher längst selbst zu Waren geworden: Vorlieben, Ansichten und Einschätzungen werden systematisch gesammelt und in Profilen zusammengefasst. Algorithmen entscheiden damit nicht nur, welche Werbung der Nutzer zu sehen bekommt, sondern wer welchen Preis für ein bestimmtes Produkt zahlen soll, wer eine bestimmte Information erhält, wer welchen Versicherungstarif, Studienplatz oder Job erhält. Verbraucher zahlen also mit Daten, wissen aber nicht, wie viel und an wen, können das Geld nicht verwalten, nicht sparen oder die Geldströme sehen. In der digitalen Welt sind Nutzerdaten das Geld – über das keine Institution mit entsprechenden Kapazitäten und Kompetenzen wacht. Der digitale Markt krankt damit an Transparenz, Kontrolle und Aufsicht. Einzig die Unternehmen bestimmen den Preis der Daten, den Verbraucher für ihre Dienste zahlen sollen.

Verbraucherfreundliche europäische Datenschutzregeln

Die Europäische Union strebt derzeit mit der Allgemeine Datenschutzverordnung eine Verbesserung des Umgangs mit Nutzerdaten an, damit Verbraucher den technischen Systemen und dahinter liegenden Geschäftsprozessen wieder vertrauen. Der Schutz persönlicher Daten hat einen hohen Stellenwert, den es zu wahren gilt. Für Unternehmen muss es strenge Regeln geben, wie mit den Daten der Verbraucher umgegangen werden darf. Klare Transparenzverpflichtungen, Einwilligungsregelungen und durchsetzbare Auskunfts- und Löschrechte sind ein Mindestmaß an Verbraucherdatenschutz, den es umzusetzen gilt. Ein europaweit einheitliches Datenschutzrecht ist dafür dringend notwendig, denn genauso wie die digitale Welt keine Landesgrenzen kennt, muss auch der Datenschutz länderübergreifend gelten. Die europäische Allgemeine Datenschutzverordnung soll daher für alle Unternehmen gelten, die in Europa Geschäfte machen, unabhängig davon, wo sich die Datenserver befinden. Wer auf dem europäischen Markt seine Dienste und Technologien anbietet, muss sich an europäisches Datenschutzrecht halten. Mit dieser Regelung würden Datenoasen wie in Irland, wo das Datenschutzrecht oft verbraucherunfreundlich ausgelegt wird, der Vergangenheit angehören – ein großer Gewinn für die Verbraucher.

Für einen starken Verbraucherdatenschutz reichen aber nicht nur starke Regelungen aus. Auch die Durchsetzung der Regelungen muss effektiv sein. Datenschutzverstöße müssen für Unternehmen spürbar sein und dürfen nicht einfach aus der „Portokasse" bezahlt werden. Die vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments vorgeschlagene Maximalstrafe von bis zu 5 Prozent des weltweiten Jahresumsatzes muss daher in den weiteren Verhandlungen beibehalten werden. Zudem sollten die Bußgelder in Ausnahmenfällen bei besonders schwerwiegendem Datenmissbrauch auch überschritten werden können.

Informationsdefizite ausgleichen

Die technischen Systeme und Geschäftsprozesse zur Datenerhebung,

-verknüpfung und -nutzung sind heute zu komplex, als dass sie von Verbrauchern durchschaut werden könnten. Die Nutzer können nicht mehr überblicken, wo auf der Welt ihre Daten gespeichert sind, welche Wege sie gehen, wer auf die Daten Zugriff hat und mit welchen anderen Datenbeständen sie verknüpft werden. Zusätzlich erhalten Verbraucher häufig auch keine oder nur unzureichende Informationen über die Datenverarbeitung, so dass sie ihren Umfang nicht einschätzen können. Aus diesen Gründen können Verbraucher oftmals keine informierte Einwilligung zur Datennutzung mehr geben oder ihre Rechte wahrnehmen, z.B. auf Auskunft oder Löschung der Daten. Zur Selbstbestimmung und Eigenverantwortung der Verbraucher zählt aber auch, dass sie selbst entscheiden können müssen, wem sie ihre Daten und für welche Zwecke sie diese anderen zur Verfügung stellen.

Damit Verbraucher wieder auf Augenhöhe mit Internet-Unternehmen agieren können, muss das Informationsungleichgewicht zu Gunsten der Verbraucher aufgelöst werden. Bisher wird versucht, mit einem “Mehr“ an Informationspflichten den Risiken, die Verbraucher im Netz ausgesetzt sind, entgegen zu wirken. Im Internet sind Allgemeine Geschäftsbedingungen und Datenschutzbestimmungen das zurzeit gängigste Mittel der Information für die Verbraucher. Diese sind jedoch in der Regel zu lang, umständlich juristisch formuliert und schwer verständlich. Und auf Mobiltelefonen gar nicht erst zu lesen. Viele Nutzer verstehen bzw. lesen die für den Vertragsschluss wichtigen Bestimmungen also nicht. Vorschnell werden die Bestimmungen durch Anklicken akzeptiert und so zum Vertragsinhalt – mit zum Teil weitreichenden Folgen: So findet sich oft im Kleingedruckten, dass persönliche Informationen an Dritte weitergegeben werden. Würde der Anbieter aber Klartext reden, träfe so mancher Nutzer vielleicht eine andere Wahl, würde also zum Beispiel einen anderen Messenger wählen oder woanders online einkaufen. Verbrauchern müssen daher endlich von den Anbietern wesentliche Informationen, die dem Medium angemessen gestaltet sind, erhalten, die sie auch tatsächlich wahrnehmen. Das gilt auch und insbesondere für Smartphones. Beispielsweise können Icons und Prüfsiegel die Informationsgestaltung im Netz unterstützen. Auch so können auf anschauliche Weise Informationen an den Verbraucher gegeben werden. Auch Verbraucherforschung kann hier einen wesentlichen Beitrag leisten. Durch unabhängige Verbraucherforschung können die Informationsbedürfnisse und Möglichkeiten der Kenntnisnahme der Verbraucher in der digitalen Welt analysiert werden. Da die Teilhabe der Verbraucher an der digitalen Welt in hohem Maße nicht nur von ihren finanziellen Ressourcen abhängt, sondern insbesondere auch von ihrer Kompetenz im Umgang mit den neuen Angeboten und Medien, muss die Forschung die verschiedenen Verbrauchertypen (verletzliche Verbraucher bis erfahrene Profis) betrachten und Lösungsvorschläge daraufhin überprüfen. Nur dann wird der Verbraucher effektiv in der Lage sein, eine bewusste Entscheidung am Markt für oder gegen einen Anbieter zu treffen. Das ist eine Grundvoraussetzung, damit Verbraucher mit Unternehmen auf Augenhöhe agieren können

.

Unternehmensverantwortung stärken

Und auch die Unternehmen selbst sollten ein größeres Interesse an einem starken Verbraucherdatenschutz entwickeln, denn nur so kann das Risiko verringert werden, dass Verbraucher sich den technischen Systemen und dahinter liegenden Geschäftsprozessen ausgeliefert fühlen. Der verantwortungsvolle Umgang mit den Daten der Nutzer, Offenheit und Transparenz bei der Erhebung und Verwertung sensibler Daten müssen die oberste Maxime für Unternehmen sein. Personenbezogene Daten dürfen nicht genutzt werden ohne Einwilligung der Betroffenen und ohne Zweckbindung. Sie müssen mitbestimmen können, ob und in welcher Form ihre Daten erfasst, zusammengeführt und genutzt werden.

Christoph Schäfer

Datenschutz und Werbung – die Froschperspektive des Düsseldorfer Kreises

Der Datenschutzbeauftragte fühlt sich manchmal wie der natürliche Feind der Marketing- und Vertriebsabteilungen. Dabei ist auch ihm klar, dass die werbliche Ansprache von (potentiellen) Kunden ein wichtiges Element zur Umsatzsicherung darstellt. Es darf allerdings dennoch nicht vergessen werden, dass die Gerichte und der Gesetzgeber zunehmend strengere Vorgaben für die Werbung machen. Auch die Datenschutz-Aufsichtsbehörden entdecken das Thema Werbung zunehmend als Betätigungsfeld – jedoch sollten sie etwas grundsätzlicher vorgehen.

1. Ansichten eines Frosches

Die Ad-hoc Arbeitsgruppe „Werbung und Adresshandel" des Düsseldorfer Kreises, dem informellen Austausch-Gremium der Datenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich, hatte bereits im November 2012 seine – nicht sehr werbewirksam benannten – „Anwendungshinweise zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke"[1] veröffentlich. Im Dezember 2013 wurde nun eine neue Version veröffentlich, die immerhin von acht auf zwölf Seiten angewachsen ist.

Wer nun meint, auf diesen zwölf Seiten ein umfassendes Skript zum Datenschutz im Zusammenhang mit Werbung zu erhalten, sollte sich nicht zu früh freuen. Es handelt es sich eher um eine lose Sammlung von aufsichtsbehördlichen Aussagen zu Einzelfragen des Datenschutzes und der Werbung. Hilfreich wäre zumindest ein diesbezüglicher Hinweis, der den unbedarften Leser vor allzu hohen Erwartungshaltungen an das Dokument schützt.

Um Missverständnisse zu vermeiden: Als Datenschützer ist man grundsätzlich dankbar für jede Aussage einer Aufsichtsbehörde, die einem Rechtssicherheit in Auslegungsfragen des Datenschutzes gibt, auch wenn sie nur wiedergibt, was Richter längst entschieden haben. Das vom Düsseldorfer Kreis vorgelegte Dokument sollte allerdings mit Vorsicht behandelt werden, da es sehr viele entscheidende Aspekte nicht behandelt und mitnichten dabei hilft, das umfassende Spannungsfeld von Datenschutz und Werbung zu erfassen. Anstatt einen Überblick aus der Vogelperspektive zu wagen, setzt man eher auf die Darstellungen aus Sicht des Frosches.

2. Das Salz der Aufsichtsbehörden

Ärgerlich ist vor allem der sträflich kurz abgehandelte Teil zur Einwilligung (Abschnitt 2.), der zudem zusammen mit Abschnitt 4.5 (zusammengefasste Einwilligungen) gelesen werden muss. Leider wird hier das komplexe Thema der Einwilligung nur sehr rudimentär behandelt, obgleich sie, wenn es um die Legitimation von Werbung geht, allzu oft als das Allheilmittel angesehen wird. An der Umsetzung einer rechtskräftigen Einwilligung scheitern dabei viele, ob nun in elektronischer oder schriftlicher Form. Die Verfasser streuen die Einwilligung nun wie Salz in ihre Arbeitshilfe – und leider manchmal auch in die Augen des Lesers.

2.1. Gültigkeit einer Einwilligung

Leider weist der Düsseldorfer Kreis nur darauf hin, dass die Gestaltung der Einwilligung „verständlich und konkret" sein muss. Darüber, was dies in den Augen der Aufsichtsbehörden konkret bedeutet, wird der Werbende weiter im Dunkeln gelassen. Einige Beispiele hätten hier vielleicht geholfen.

Wenigstens wurde erkannt, dass die Frage, wie lange eine einmal erteilte Einwilligung ihre Gültigkeit hat (Abschnitt 2.2), äußerst spannend ist. Leider wird aber trotzdem lediglich ein einsames Urteil des LG München I vom 08.04.2010 (Az. 17 HK O 138/10) ausgewertet, in welchem eine 17 Monate lang „ungenutzte" Einwilligung zur E-Mail-Werbung als ungültig angesehen wird. Ähnliches hatte das LG Berlin allerdings schon 2004 entschieden (Az. 15 O 653/03), auch wenn es dort noch um 24 Monate ging. Vielmehr als eine exemplarische Urteilsnennung wäre eine Positionierung der Aufsichtsbehörden zur Frage der Gültigkeitsdauer einer Einwilligung wünschenswert gewesen.

2.2. Einwilligung per Visitenkarten

Spannend ist die Auseinandersetzung im Abschnitt 4.1 mit der Frage, inwiefern die Übergabe einer Visitenkarte eine Einwilligung in die Zusendung von Werbung darstellt. Gerade für Unternehmen, die eine hohe Präsenz auf Messen haben, stellt dies einen nicht unwesentlichen Punkt dar. Bisher hat der praktisch beratende Datenschützer wohl meist Fragebögen empfohlen, an die die Visitenkarte angeheftet wird, und die man sich schließlich vom Interessenten abzeichnen lässt – natürlich mit entsprechender Formulierung zur Werbe-Einwilligung. Nun postulieren die Datenschutz-Aufsichtsbehörde, dass die reine Übergabe der Visitenkarte bereits eine rechtswirksame Einwilligung darstellen kann.

Wohlgemerkt „kann", denn ganz festlegen will man sich hier wohl nicht. Besser ist das auch, denn das LG Baden-Baden hat unlängst entschieden (Urteil vom 18.01.2012, Az. 5 O 100/11), dass die Übergabe einer Visitenkarte zumindest nicht die nach § 7 Abs. 2 Nr. 3 UWG erforderliche ausdrückliche Zustimmung zum Empfang von Werbe-E-Mails darstellt. Das heißt natürlich nicht, dass man als Vertriebler den Interessen-

ten, der einem auf der letzten Messe seine Visitenkarte übergeben hat, nicht anschließend persönlich kontaktieren darf. Aber die Aufnahme in die zentrale CRM-Datenbank (wohl noch vertretbar) mit folgender Versorgung mit einem wöchentlichen E-Mail-Newsletter oder gar telefonischer Kontaktaufnahme durch den Callcenter-Dienstleister ist angesichts der bestehenden Rechtslage sicher nicht die beste Idee. Um hier angesichts entgegenstehender Rechtsprechung Rechtssicherheit zu schaffen, ist die Darstellung viel zu knapp begründet.

3.2. Double Opt-in als Herausforderung

Um beim heiß umkämpften Thema der elektronisch versendeten Werbung zu bleiben, beschäftigt sich der Abschnitt 4.4 mit dem sogenannten Double Opt-in-Verfahren. Nachdem man sich früher noch per einfachem Kontaktfeld einen E-Mail-Newsletter bestellen konnte, hat sich hierbei inzwischen das Double Opt-in-Verfahren durchgesetzt. Dabei sendet der Interessent seine E-Mail-Adresse per Kontaktfeld an den Werbe-Anbieter, der wiederum einen Anmelde-Link zur Aktivierung des Newsletter-Versandes versendet. Dies soll verhindern, dass bei gewollter oder ungewollter Fehleingabe der E-Mail-Adresse unerwünschte Werbe-E-Mails versendet werden. Spam ist schließlich inzwischen kaum noch jemandem als fragwürdige Leckerei bekannt, sondern nervt vielmehr beim täglichen Bereinigen des überquellenden E-Mail-Postfaches.

Für Aufsehen sorgte das OLG München, welches mit seinem Urteil vom 27.09.2012 (Az. 29 U 1682/12) feststellte, dass auch bereits die Versendung des Anmelde-Links an einen unbeteiligten Empfänger eine unerwünschte Werbung darstellt. Die vermeintlich überraschende Entscheidung war nur eine logische Anwendung des Gesetzes – denn eine unverlangte E-Mail bleibt eine unverlangt E-Mail, deren Werbegehalt angesichts der angestrebten Kundenbindung durch den Newsletter und des Bestrebens, Interesse zu wecken, in der Regel nicht zu leugnen ist. Das OLG bietet als Ausweg an, dass man das Verlangen der E-Mail durch den E-Mail-Empfänger nachweisen muss, und beschreibt:

„Für den Nachweis des Einverständnisses ist es erforderlich, dass der Werbende die konkrete Einverständniserklärung jedes einzelnen Verbrauchers vollständig dokumentiert. Im Fall einer elektronisch übermittelten Einverständniserklärung setzt das deren Speicherung und die jederzeitige Möglichkeit voraus, sie auszudrucken. Die Speicherung ist dem Werbenden ohne Weiteres möglich und zumutbar.“

Vermutlich in Unkenntnis dieses neueren Urteils beziehen sich die Anwendungshinweise auf ein BGH-Urteil vom 10.02.2011 (I ZR 164/09). Erkannt – weil im Urteil genannt - wurde jedenfalls, dass das bloße Abspeichern der „IP-Adresse des Anschlusshinhabers“ nicht genügt, um den Nachweis zu führen. Richtig, welche Aussage sollte diese auch haben, wenn das Kontaktformular im offenen WLAN-Netz eines Schnellrestaurants oder am Bahnhof ausgefüllt wurde. Einen Hinweis darauf, welche Informationen erforderlich sind, um erfolgreich den Nachweis des Werbevelangens zu führen, bekommt der geneigte Leser leider nicht geliefert. Dies dürften nämlich zumindest noch der Zeitpunkt der Anmeldung, der Inhalt der Bestätigungs-E-Mail, der Zeitpunkt der Bestätigung sowie die IP-Adresse des Bestätigenden sein.

Als Nachweis der Einwilligung fordert der Düsseldorfer Kreis – in Anlehnung an das BGH-Urteil - „z. B. den Ausdruck einer E-Mail des Betroffenen mit der entsprechenden Willenserklärung“. Wenn auch die Richter hier schon eine spannende Anforderung gestellt haben, so wäre es doch vermutlich nicht zu viel erwartet gewesen, wenn sich die Aufsichtsbehörde mit der Frage beschäftigt hätte, welchen Beweiswert der Ausdruck einer E-Mail haben sollte. Vielmehr ist hier der Aufbau einer Datenbank mit entsprechender Speicherung von Übermittlungsvorgängen mit Zeitstempeln anzuraten.

Abschließend wird zumindest noch erklärt, dass das Double-Opt-in-Verfahren für die Einwilligung in Werbe-Anrufe nicht funktionieren kann, weil: „Mit der Übersendung einer Bestätigungs-E-Mail kann nämlich der Nachweis der Identität zwischen dem die Einwilligung mittels E-Mail Erklärenden und dem Anschlussinhaber der Telefonnummer nicht geführt werden.“ Diese erhellende Erkenntnis muss man wohl einfach so stehen lassen

3. Die Einwilligung im Überblick

In den letzten Jahren kann man eine immer strenger werdende Tendenz ober- und höchstrichterlicher Rechtsprechung hinsichtlich der formalen und inhaltlichen Anforderungen an Einwilligungserklärungen feststellen. Hinweise auf die zu kleinen Schriftgrößen, auf die unzulässige Koppelung mit anderen Erklärungen sowie die Forderung nach einer möglichst konkreten Zweckbestimmung entsprechen damit der gängigen Meinung der Gerichte.

Es gilt stets, sowohl das Datenschutz- als auch das Wettbewerbsrecht im Auge zu behalten. Außerdem muss man unterscheiden, ob man Endkunden (Verbraucher) oder Geschäftskunden bewerben will - bei Verbrauchern liegen die Hürden nochmals deutlich höher.

3.1. Wer kann einwilligen?

Ein weit verbreiteter Irrtum ist es, dass nur Volljährige in Werbung einwilligen können. Entscheidend für eine rechtskräftige Einwilligung ist allerdings nicht die Geschäftsfähigkeit, sondern die Einsichtsfähigkeit. Das OLG Hamm urteilte (Urteil vom 20.09.2012, I-4 U 85/12) allerdings, dass auch Minderjährige ab 15 Jahren nicht die nötige Reife haben (kann), die Tragweite der Einwilligungserklärung zur Datenspeicherung und Datenverwendung zu Werbezwecken abzusehen und daher die Zustimmung der Eltern ebenfalls nötig sei. Im Zweifel ist das Vorliegen der Einsichtsfähigkeit also im Einzelfall zu prüfen

.

3.2. Arten von Einwilligungen

Man unterscheidet die ausdrückliche Einwilligung (z. B. durch das Ankreuzen eines Feldes „[ ] Ja, ich willige ein…“), die konkludente Einwilligung (durch schlüssiges Verhalten) und die mutmaßliche Einwilligung (aufgrund konkreter Umstände kann ein sachliches Interesse angenommen werden, z. B. bei Telefonwerbung bei Geschäftskunden).

3.3 Einwilligungen nach dem Datenschutzrecht

3.3.1. Schriftliche Einwilligung

Das Bundesdatenschutzgesetz (BDSG) verlangt, dass eine Einwilligung stets

freiwillig erfolgen und man darüber informiert sein muss, in was man genau einwilligt (§ 4a Abs. 1 BDSG). Auch muss man den Kunden umfassend informieren (§ 4 Abs. 3 BDSG): Wer ist der Werbende? Für welchen Zweck bzw. für welche Zwecke werden die Daten verwendet? Wer sind die (Kategorien der) Empfänger der Daten? Hierbei spricht man vom Transparenzgebot.

Außerdem verlangt das BDSG grundsätzlich die Schriftform (§ 4a Abs. 1 BDSG) sowie die deutliche Hervorhebung der Einwilligungserklärung, wenn sie zusammen mit anderen Erklärungen erteilt wird (das „Kleingedruckte“ ist verboten). Erhebt man besondere personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG, muss für diese Daten eine gesonderte und ausdrückliche Einwilligung eingeholt werden (§ 4 Abs. 3 BDSG).

3.3.2. Elektronische Einwilligung

Ein Sonderfall ist die elektronische Einwilligung, die beispielsweise auf Internetseiten oder in Apps für mobile Geräte genutzt wird. Diese richtet sich sowohl nach dem BDSG (§ 28 Abs. 3a BDSG), als auch nach dem Telemediengesetz (§ 13 Abs. 2 TMG).

Für die elektronische Einwilligung gelten die folgenden Voraussetzungen: Der Nutzer (Betroffene) muss bewusst und eindeutig einwilligen (z. B. Mausklick in ein hervorgehobenes Feld am Bildschirm), den Inhalt der Einwilligung jederzeit abrufen können, seine Einwilligung jederzeit widerrufen können. Der Diensteanbieter (z. B. Betreiber der Internetseite) muss die Einwilligung protokollieren (siehe oben), den Nutzer vor der Erklärung der Einwilligung auf sein Widerrufsrecht hinweisen und den Widerrufshinweis jederzeit abrufbar machen.

Außerdem gibt es – ähnlich der schriftlichen Einwilligung – umfangreiche Informationspflichten. Der Diensteanbieter muss den Nutzer vor Beginn der Nutzung über die Art, den Umfang und den oder die Zweck(e) der Datenverarbeitung sowie eventuelle Datenverarbeitung außerhalb der EU/ EWR hinweisen (§ 13 Abs. 1 TMG), was gerade bei der Verwendung von Social Media-Buttons problematisch ist.

3.3.3. Telefonische Einwilligung (auch Fax/ E-Mail)

Auch die telefonische Einwilligung ist möglich. Ein Werbeanruf liegt auch dann vor, wenn in dem Anruf (nur) nach einem Interesse an Werbung gefragt wird. Daher ist auch für einen solchen Anruf eine Einwilligung erforderlich, wie unter anderem das LG Leipzig in seinem Beschluss vom 09.10.2009 feststellte (Az. 05 O 3424/09). Das LG Bochum stellte mit seinem Urteil vom 05.05.2008 (Az. 14 O 61/08) fest, dass es ist nicht wettbewerbswidrig ist, wenn Anrufer konkret gefragt werden, ob sie damit einverstanden sind, dass ihre Daten für spätere werbliche Zwecke genutzt werden. Man muss dem Anrufer allerdings seine Einwilligung schriftlich bestätigen (§ 28 Abs. 3a BDSG). Dies kann durch einen gesonderten Brief, aber auch z. B. durch einen Hinweis auf einer Rechnung erfolgen. Hierzu genügt keine E-Mail oder Fax, da diese nicht die Schriftform erfüllen. Auch bei Einwilligungen per E-Mail oder Fax muss eine schriftliche Bestätigung erfolgen.

3.4. Einwilligungen nach dem Wettbewerbsrecht

Neben den datenschutzrechtlichen Vorgaben muss auch das Wettbewerbsrecht beachtet werden - hierzu muss man in das Gesetz gegen den unlauteren Wettbewerb (UWG) schauen.

Das UWG schreibt vor (§ 7 Abs. 2 und 3 UWG), dass der Beworbene vor der Zusendung von Werbung ausdrücklich in die Zusendung eingewilligt haben muss. Eine Ausnahme stellt lediglich das Telefonmarketing gegenüber Geschäftskunden dar. Ein Schriftformerfordernis sieht das UWG nicht vor, die Schriftform ist aber schon aus Beweisgründen anzuraten.

3.4.1. Werbung per E-Mail oder Fax

Die Werbung per E-Mail oder Fax kann eine sogenannte „unzumutbare Belästigung“ im Sinne des UWG darstellen (z. B. Spam-E-Mails). Das ist immer dann der Fall, wenn vorher keine ausdrückliche Einwilligung erfolgt ist (§ 7 Abs. 2 Nr. 3 UWG). Eine Zuwiderhandlung kann zu Bußgeldern und Abmahnungen führen.

Die Veröffentlichung von Kommunikationsdaten (z. B. auf einer Internetseite) stell keine ausdrückliche Einwilligung in E-Mail- oder Fax-Werbung dar, wie das LG Kleve mit seinem Urteil vom 09.03.2010 (Az. 7 O 38/08) feststellte. Auch der Eintrag der Faxnummer in einem öffentlichen Verzeichnis (z. B. Telefonbuch) stellt keine Einwilligung in Werbung dar (LG Ulm, Urteil vom 30.04.2009, Az. 10 O 39/09).

3.4.2. Anforderungen an die Einwilligung

Wichtig ist, dass die Einwilligung in E-Mail- bzw. Fax-Werbung stets gesondert eingeholt werden muss. Es muss also z. B. für diese beiden Werbewege ein separates Ankreuzfeld auf einer Gewinnspiel-Postkarte geben, wie der BGH mit seinem Urteil vom 16.07.2008 klarstellte (Az. VIII ZR 348/06).

Häufig sind z. B. bei einer Bestellung auf einer Internetseite umfangreiche Formularfelder vorgesehen. Allein der Eintrag der E-Mail-Adresse in solche Felder gilt noch nicht als Einwilligung für Werbung (BGH, Beschluss vom 10.12.2009, Az. I ZR 201/07). Außerdem muss es sich um aktives Ankreuzen (Opt-in) handeln. Ein vorangekreuztes Feld (Opt-out), welches man zuerst streichen bzw. abhaken müsste, erfüllt nicht die Anforderungen an eine Einwilligung (OLG Thüringen, Urteil vom 21.04.2010, Az. 2 U 88/10).

3.4.3. Newsletter-Funktion auf Internetseiten

Ein Sonderfall, dem in der Praxis eine hohe Bedeutung zukommt, ist der E-Mail-Newsletter. Hierbei ist es regelmäßig so, dass man seine E-Mail-Adresse in ein Formularfeld eintragen kann, um hiernach einen Newsletter per E-Mail zu bekommen. Allerdings darf man als Unternehmen dann nicht direkt den Newsletter lossenden.

Vielmehr bedarf es einer Bestätigungs-E-Mail an die eingetragene E-Mail-Adresse. Hierbei muss der Empfänger entweder einen Link anklicken, oder aber einen zugesandten Code eingeben, um sich endgültig für den Newsletter anzumelden - dies nennt man „Double Opt-in“.

Hintergrund dieser Regelung ist die Authentifizierung des E-Mail-Inhabers – schließlich könnte jeder einfach die E-Mail-Adresse, auch ohne Wissen des

Anschlussinhabers, eingetragen haben. Die Bestätigungs-E-Mail gilt dann nicht als unzumutbare Belästigung, auch wenn ein Dritter die Adresse eingetragen hatte (LG München I, Beschluss vom 13.10.2009, Az. 31 T 1436/09).

3.4.4. Werbung per Telefon

Das UWG regelt, dass eine „unzumutbare Belästigung" bei einem Telefonanruf immer anzunehmen ist, wenn nicht zumindest eine „mutmaßliche Einwilligung" vorliegt. Dabei genügt nicht nur ein allgemeiner Sachbezug (BGH, Urteil vom 16.11.2006, Az. I ZR 191/03). So kann beispielsweise ein Anbieter von Kopiergeräten nicht argumentieren, dass er einen Arzt anrufen darf, da Ärzte grundsätzlich ein Kopiergerät benötigt.

Vielmehr muss nach Auffassung des OLG Celle (Beschluss vom 29.04.2010, Az. 13 U 189/09) eine sogenannte Branchenüblichkeit gegeben sein. Daher kann ein Medizintechnikhersteller – im Gegensatz zum Kopiergerätehersteller – die mutmaßliche Einwilligung in einen Werbeanruf bei einem Arzt durchaus unterstellen.

Das OLG München stellte fest (Beschluss vom 14.09.2007, Az. 6 W 622/07), dass bei der telefonischen werblichen Ansprache von Verbrauchern immer eine schriftliche Einverständniserklärung vorliegen muss. Wie auch oben schon erwähnt, genügen dabei weder E-Mail noch Fax, da diese nicht die gesetzliche Schriftform erfüllen.

An die Telefonwerbung gegenüber Verbrauchern setzen vor allem die Gerichte hohe Anforderungen. So darf man private Kunden zu Werbezwecken stets nur mit deren vorheriger Einwilligung anrufen, auch wenn sie schon ähnliche Produkte erworben haben (OLG Köln, Urteil vom 25.02.2005, Az. 6 U 155/05; OLG Frankfurt, Urteil vom 21.07.2005, Az. 6 U 175/04; OLG Braunschweig, Urteil vom 16.12.2008, Az. 2 U 9/08; OLG Köln, Urteil vom 05.06.2009, Az. 6 U 1/09).

Bei Werbeanrufen gegenüber Verbrauchern ist der Anrufer für die Behauptung, der Verbraucher sei mit dem Anruf einverstanden gewesen (LG Hamburg, Urteil vom 23.12.2008, Az. 312 O 362/08), beweispflichtig. Man muss die Einwilligung also dokumentieren. Die Datenschutzaufsichtsbehörde Baden-Württemberg hat in Ihrem Tätigkeitsbericht von 2007 festgestellt, dass die Einwilligungserklärungen in Papierform oder auf Mikrofilm aufbewahrt werden müssen, solange von ihnen Gebrauch gemacht wird.

3.4.5. Schriftliche Werbung

Die postalische Werbung gegenüber Geschäftskunden ist grundsätzlich relativ unproblematisch. Der BGH hat bereits vor geraumer Zeit entschieden (Urteil vom 16.02.1973, Az. I ZR 160/71), dass die Gefahr einer unzumutbaren Belästigung bei schriftlicher Werbung erheblich geringer ist, als es bei elektronischer Werbung der Fall ist. Will man einen Verbraucher postalisch bewerben, benötigt man dessen Einwilligung.

4. Der dumme Verbraucher

In der Praxis stellt das Verwalten und Umsetzen von Werbewidersprüchen immer wieder eine Herausforderung dar. Während dies bei der Benutzung einer zentralen CRM-Software noch relativ leicht zu handhaben ist, stoßen die Jongleure von Excel-Arbeitsmappen dabei schnell an ihre Grenzen.

Die Aufsichtbehörden jedenfalls bestätigen in Abschnitt 5.1 für den Fall eines Werbewiderspruchs die (logische) Notwendigkeit des Vorhaltens eines Namens samt Kontaktdaten des Werbeunwilligen im Rahmen einer Sperrdatei (§§ 28 Abs. 1 S. 1 Nr. 2 i. V. m. 28 Abs. 4 BDSG). Über die Aufnahme in eine solche Sperrdatei (auch Robinsonlisten genannt) soll der Werbende als verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG den Werbeunwilligen alsdann informieren. Widerspricht der Betroffene dem und verlangt, dass seine Daten wirklich gelöscht werden, muss ihn die verantwortliche Stelle dann aber informieren, dass es ihm passieren kann, dass er in der Folge wieder Werbe-E-Mails bekommen kann.

Gerade am letzten Beispiel über das Vorgehen bei der Verwaltung einer Sperrdatei lässt sich veranschaulichen, dass die Datenschutz-Aufsichtsbehörden das Vorhandensein des gesunden Menschenverstandes beim Betroffenen gelegentlich vollständig ausschließen und ihnen manchmal der Blick für das Wesentliche fehlt. Jedenfalls hätte man eine so umfassende und detaillierte Beschreibung eines datenschutzkonformen Vorgehens vielleicht eher an manch anderer Stelle des Dokuments erwartet oder sich wenigstens gewünscht . Gerade im Beratungsalltag als Datenschützer ist man bei der Auslegung des Gesetzes allzu oft auf sich allein gestellt. Es gibt viel zu wenige konkrete Aussagen der Aufsichtsbehörden und viel zu viele von der Art, die nur den Gesetzestext wiedergeben – aber lesen können wir doch alle selbst.

5. Fazit

Unser Dank gilt dem Düsseldorfer Kreis. Und das ist ernst gemeint, denn es gibt bislang noch viel zu wenige „Leitfäden" für die Auslegung des Datenschutzrechts. Allerdings darf nicht unerwähnt bleiben, dass Papiere wie das vorliegende nur wenig hilfreich sind, solange sie nur eine Ansammlung von Einzelentscheidungen und Ansichten darstellen. Damit ist dem Datenschutz dann eher ein Bärendienst erwiesen.

Hilfreich könnte es zudem sein, das Hoffen auf Einsicht von verarbeitenden Stellen, wie es bei mancher Aufsichtsbehörde gelegentlich vorzuliegen scheint, durch etwas deutlichere Sanktionierungen abzulösen. Schließlich ist es nicht die Aufgabe von Unternehmen, sich möglichst rechtskonform zu verhalten (die Compliance-Beauftragten unter den Lesern mögen dem Autor verzeihen). Denn informiert man schließlich den Geschäftsführer seines Unternehmens über die Bußgeldhöhe von bis zu 300.000 Euro laut § 43 Abs. 3 Satz 1 BDSG, um eine Datenschutz-Awareness herbeizuführen, hofft man doch gleichzeitig, dass er nicht nach dem konkreten Bußgeld-Risiko und der Wahrscheinlichkeit fragt.

Die verhängten Bußgelder sind zu gering und zu selten. Dabei hätten höhere und häufigere Bußgelder möglicherweise auch zur Folge, dass mehr Unternehmen die Entscheidungen von Aufsichtsbehörden durch ein Gericht überprüfen lassen. Die Ergebnisse dürften dabei spannend werden. Denn letztlich gibt es doch keinen schlechteren Zustand, als den der (rechtlichen) Unsicherheit.

1 http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Anwendungshinweise_Werbung.pdf

Ansprache von Bundesinnenminister Dr. Thomas de Maizière, MdB, anlässlich des Amtswechsels beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 04. Februar 2014

Sehr geehrte Frau Voßhoff,
sehr geehrter Herr Schaar,
ich begrüße die Mitglieder des Deutschen Bundestages sowie die anwesenden Datenschutzbeauftragten der Länder,
sehr geehrte Damen und Herren,

das Amt des Bundesbeauftragten für Datenschutz und Informationsfreiheit nimmt – verwaltungsorganisatorisch gesehen – eine Sonderstellung ein.

Eingerichtet beim Bundesinnenministerium ist sie dennoch an keine Fachaufsicht gebunden. Sie agiert vielmehr unabhängig und ist letztlich nur dem Gesetz verpflichtet. Diese Unabhängigkeit ist rechtlich geboten und das ist auch gut so.

Effiziente und nachhaltige Kontrolle, datenschutzrechtliche Kontrolle der Bundesbehörden und anderer öffentlichen Stellen wäre anders nicht möglich.

Sie, Herr Schaar, haben einmal behauptet: „Das Amt formt den Menschen." Damit mögen Sie recht haben.

Indem Sie nicht müde wurden, kritisch zu hinterfragen, Vorbehalte äußerten – sei es nun an der Videoüberwachung, der Anti-Terror-Datei oder der Online-Durchsuchung – sind Sie Ihrem Anspruch an Ihr Amt vollumfänglich gerecht geworden. Sie haben sich als Hüter des Datenschutzes vehement für den Schutz der Privatsphäre und gegen Datenmissbrauch ausgesprochen.

Nicht immer haben Sie sich durchgesetzt. Nicht immer waren Sie mit der Bundesregierung und der Bundestagsmehrheit einer Meinung. Aber auch das ist gut so.

Seit Sie das Amt des Bundesbeauftragten am 17. Dezember 2003 übernommen haben, gab es viele Gelegenheiten, nachdrücklich für den Datenschutz Position zu beziehen. Neben der Sicherheitsgesetzgebung nach den Terroranschlägen in den USA war das vor allem auch der rasante technische Fortschritt im Bereich der IT.

Und immer auch haben diese Ereignisse und Maßnahmen Auswirkungen auf den Datenschutz. Das haben Sie stets deutlich gemacht und dadurch die Entwicklung des Datenschutzes nachhaltig geprägt, ihm zur öffentlichen Wahrnehmung und Resonanz verholfen.

In Ihrer Amtszeit ist Ihnen - mit Inkrafttreten des Informationsfreiheitsgesetzes zum 1. Januar 2006 - auch die Aufgabe des Informationsfreiheitsbeauftragten übertragen worden. Damit haben Sie in den zurückliegenden acht Jahren die Kontroll- und Ombudsfunktion für die Bereiche Datenschutz und Informationsfreiheit in Personalunion wahrgenommen. In dieser neuen Funktion haben Sie sich intensiv für eine Stärkung und Ausweitung des Zugangs zu amtlichen Informationen eingesetzt und sich für eine Intensivierung der behördlichen Transparenz stark gemacht.

Sehr geehrter Herr Schaar, im Namen der gesamten Bundesregierung danke ich Ihnen für Ihren großen Einsatz für den Datenschutz und die Informationsfreiheit. Ich bin sicher, dass Sie auch künftig die Entwicklung dieser Bereiche kritisch begleiten. Herzlichen Dank!

Ihnen, Frau Voßhoff, gratuliere ich zur Übernahme Ihres neuen Amtes als Datenschutzbeauftragte und wünsche Ihnen viel Erfolg für Ihre künftige Arbeit.

Am 19. Dezember 2013 hat der Deutsche Bundestag Sie als neue Bundesbeauftragte für den Datenschutz und die Informationsfreiheit gewählt. Sie genießen damit eine Legitimation, die Ihrem Amt und Ihrer Stimme in unserer demokratischen Gesellschaft ein besonderes Gewicht verleiht.

Ich freue mich, dass es gelungen ist, eine so erfahrene und anerkannte Juristin für dieses Amt zu gewinnen.

Ihr Amtsantritt fällt in eine Zeit, in der einerseits unter dem Eindruck der Enthüllungen eines Edward Snowden darüber gestritten wird, wie Datenschutz auch gegenüber geheimdienstlichen Aktivitäten verteidigt werden kann, in der aber andererseits auch an einem Projekt gearbeitet wird, das für uns alle Maßstäbe setzen wird: Die Schaffung eines an den Erfordernissen einer modernen Welt ausgerichteten Datenschutzrechts – die Arbeit an der EU-Datenschutz-Grundverordnung.

Die globale Vernetzung stellt uns vor neue Herausforderungen. Durch das Internet erhalten die geltenden Regelungen eine neue Dimension. Phänomene wie Cloud-Computing, Google oder Facebook waren bei Erlass der geltenden Datenschutzrichtlinie im Jahre 1995 noch kaum vorstellbar.

Um die durch die Nutzung des Internets entstandenen neuen Risiken zu minimieren und gleichzeitig die Chancen der Digitalisierung zu wahren, brauchen wir ein neues modernes Datenschutzrecht, das hohe Schutzstandards international absichert.

Deshalb hat der Entwurf einer europäischen Datenschutz-Grundverordnung hohe Priorität.

Nur gemeinsam wird es uns gelingen, ein wirklich zukunftsfähiges Regelwerk zu schaffen. Wir müssen die Chance nutzen, mit der Datenschutz-Grundverordnung ein Regelwerk zu machen, das auch den Herausforderungen von Cloud-Computing, Sozialen Netzwerken oder sogenannten Wearables gerecht wird.

Wir brauchen auch Antworten auf die neuen technischen Entwicklungen.

Ich verstehe all diejenigen, die sich

einen raschen Abschluss der Arbeiten wünschen. Wir beteiligen uns aktiv an den Beratungen. Ich sage nur: die Qualität muss stimmen.

Dazu gehört auch, sich stark auf das zu konzentrieren, was auf Europäischer Ebene unbedingt geregelt werden muss - nämlich Google, Facebook und Co. Ein „One-Size-Fits-All"-Modell kann dem schnellen Abschluss der Verhandlungen in Brüssel entgegenstehen. Die Datenschutzbeauftragten in Deutschland werden sich vermutlich schwer tun, die zum Teil deutlich strengeren und differenzierteren Datenschutzbestimmungen im öffentlichen Bereich einer Vollharmonisierung zu opfern.

Das alles ist nicht unlösbar. Wir können auch nicht verlangen, dass sich die ganze Europäische Union nach unserem Datenschutzrecht ausrichtet. Aber es braucht eben etwas mehr konkrete Arbeit an Texten und damit etwas mehr Zeit.

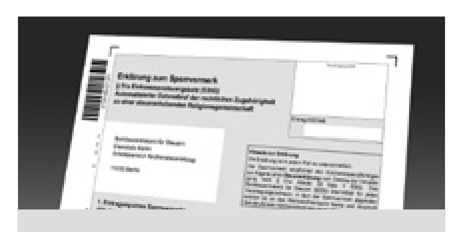
Aber nicht nur international sehe ich Handlungsbedarf. Wichtige Themen bei uns sind die Ausgestaltung der Unabhängigkeit der Bundesbeauftragten für den Datenschutz und die Zusammenarbeit der deutschen Datenschutzaufsichtsbehörden untereinander. Ich würde mich freuen, wenn hierzu gemeinsame Vorschläge entwickelt werden könnten.

Ich gehe davon aus, dass es auch künftig zwischen der Datenschutzbundesbeauftragten und den Bundesbehörden Meinungsunterschiede hinsichtlich der Auslegung von Regelungen des Datenschutzes oder der Ausnahmetatbestände des Informationsfreiheitsgesetzes geben wird. Angesichts der unterschiedlichen Interessenlagen werden auch mögliche Überlegungen für eine Weiterentwicklung dieser Rechtsbereiche kontrovers verlaufen.

Aber wie bereits gesagt: Es gehört zur Arbeit einer Kontrollstelle, kritisch und unabhängig zu beurteilen, was sie im Rahmen ihrer Kontrolltätigkeit vorfindet.

Im demokratischen Rechtsstaat ist die gegenseitige Achtung vor der jeweiligen Funktion ein hohes Gut, das es zu wahren gilt. Unser Staatswesen baut darauf auf. Diese Balance ist umso fruchtbarer, je unaufgeregter sie praktiziert wird. Dazu sollten wir alle gemeinsam beitragen.

Sehr geehrte Frau Voßhoff, ich freue mich auf eine konstruktive Zusammenarbeit.



Beantragung eines Sperrvermerks

Der Kirchensteuerabzug für Kapitalerträge soll im Regelfall ab 2015 automatisiert über die Kreditinstitute erfolgen. Dazu werden diese durch ein elektronisches Abrufverfahren die Religionszugehörigkeit ihrer Sparer beim Bundezentralamt erfahren.

Wer nicht wünscht, dass Banken, Versicherungen und Fondsgesellschaften die Religionszugehörigkeit kennen, kann dies durch einen Sperrvermerk beim Bundeszentralamt verhindern. Die eventuelle anfallende Kirchensteuer wird dann wie bisher im Rahmen der Einkommenssteuererklärung abgeführt.
Das Formular, das mit der Post geschickt werden muss, findet man hier: http://www.formulare-bfinv.de/ffw/action/invoke.do?id=010156

Hans-Hermann Schild

Zur Bestellung der Bundesbeauftragten/des Bundesbeauftragten für den Datenschutz: Vergleich und Plädoyer

Am 17.12.2013 meldete die Presse, dass die bisherige Bundestagsabgeordnete Andrea Voßhoff als Nachfolgerin von Peter Schaar in das Amt des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt werden solle.[1] Nach den letzten Erfahrungen mit Berufungen beim Bund, aber auch mit Ausschreibungen in den Bundesländern[2], wurden Personen benannt und gewählt, die zumindest in der „Community des Datenschutzes" bekannt waren. Bei der neuen Bundesbeauftragten handelt es sich nun um eine Person, welche bisher mit der Thematik vollkommen unbefasst und somit unbekannt war[3], also „ein unbeschriebenes Blatt", wie Ex-Bundesinnenminister Gerhart Baum zitiert wurde.[4]

Am 28.01.2014 konnte man lesen, dass Peter Hustinx – anders als in Deutschland – kommissarisch noch bis Mitte Oktober EU-Datenschutzbeauftragter bleiben würde, obwohl seine zweite und letzte Amtszeit am 16. Januar auslief.[5] Grund dafür sei, dass sich die Suche nach einem Nachfolger schwierig gestaltete, da das zuständige Auswahlgremium der Kommission kurz vor dem geplanten Ausscheiden des Amtsinhabers alle bisherigen Personalvorschläge für einen neuen Datenschutzbeauftragten abgelehnt habe. Zur Begründung

hieß es außerdem, dass es den Bewerbern, unter denen unter anderem Leiter und Vizechefs einschlägiger Aufsichtsbehörden in Finnland, Polen, Österreich und Ungarn waren, an „Management-Erfahrung" mangele.[6]

In Deutschland hingegen fand eine Ausschreibung durch das Bundesministerium des Innern erst gar nicht statt. Vielmehr unterbreitete das Kabinett dem Deutschen Bundestag den Wahlvorschlag, ohne dass irgendeine öffentliche Erklärung zu dem Anforderungsprofil an das Amt bekannt wurde. Demgegenüber hatte die Europäische Kommission die Stelle des Europäischen Datenschutzbeauftragten vom Amtsblatt am 31. Juli 2013[7] mit einem dezidierten Anforderungsprofil ausgeschrieben. Dies ging so weit, dass als Zulassungsbedingung für eine Bewerbung u.a. eine fünfzehnjährige Berufserfahrung und davon wiederum mindestens fünf Jahre in einer höheren Führungsposition gefordert wurde, bei der die Zahl der unterstellten Mitarbeiter, die Höhe des verwalteten Etas und der Platz der Hierarchie anzugeben waren.[8] Hierdurch wurde nicht nur ein Anforderungsprofil für das Amt festgelegt, sondern darüber hinaus eine Zugangshürde aufgebaut, die mit der Qualifikation und dem Amt nur wenig zu tun haben. Nach den allgemeinen Grundsätzen des deutschen Beamtenrechts hätten diese hohen „Zulassungsbedingungen" um sich überhaupt bewerben zu können, allenfalls zu den Hilfskriterien gehören können, die bei gleicher Qualifikation von Bewerbern zur endgültigen Auswahl herangezogen werden sollen.

Damit hat die Europäische Kommission zwar eine Ausschreibung durchgeführt und ein abgebrochenes Auswahlverfahren herbeigeführt, aber zugleich Zulassungshürden aufgebaut, die dem Amte und den eigentlichen Anforderungen an die erforderliche Qualifikation nicht gerecht wurden. Andererseits hätten das Bundesministerium des Innern und das Bundeskabinett erkennen müssen, dass nach der europäischen Datenschutzrichtlinie und der Rechtsprechung des Europäischen Gerichtshofes „Kontrollstellen" zu schaffen sind, die ihre Aufgaben nicht nur „in völliger Unabhängigkeit" wahrnehmen[9], sondern sich die damit erforderliche Stellenausschreibung auch an Art. 33 GG zu orientieren hat.[10] Handelt es sich doch und gerade bei der derzeitigen Konstruktion der „Behörde Bundesbeauftragter für den Datenschutz" im weitesten Sinne um eine „Abteilung" des Bundesinnenministeriums.

Die Problematik der fehlenden Unabhängigkeit scheint der nunmehrige Innenmister Dr. Thomas de Maizière nach seiner Rede zur Einführung der „Neuen" und Verabschiedung des „Alten" am 4. Februar 2014 erkannt zu haben. Nicht erkannt wurde jedoch, dass nach Art. 33 Abs. 2 GG jeder Deutsche nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amte hat. Da es sich vorliegend um kein politisches Amt handelt - auch wenn Fragen zum Grundrecht auf informationelle Selbstbestimmung immer im hohen Maße politisch sind - hätte hier nach den ganz allgemeinen Grundsätzen des Beamtenrechts eine Ausschreibung mit einem qualifiziertem Anforderungsprofil erfolgen müssen, wie bei jedem anderen Behördenleiter auch. Wenn aber ein Bundesministerium und der Bundesminister Selbstverständlichkeiten „vergessen", müssen diese bei der anstehenden Gesetzesänderung mit der die Unabhängigkeit der „Kontrollstelle" erreicht werden soll, ebenfalls mit aufgenommen werden.[11]

Über das letztendlich zu bestimmende Anforderungsprofil ließe sich jedoch ebenfalls streiten, es sei denn, es wird an der Aufgabe des Amtes so fixiert, wie dies die Kommission in ihrer Ausschreibung vollzogen hatte.[12] Ob im Anforderungsprofil auch die Stellung und Funktion eines Richters oder aber die Befähigung zum Richteramt gefordert werden muss, sei vorliegend dahin gestellt. Zumindest sollte die Frage aus einem der letzten Beitrittsstaaten in die Europäische Union an deutsche Datenschutzvertreter doch zu denken geben: wie viele Richter denn Datenschutzbeauftragte bzw. Mitarbeiter eines Landes-/Bundesdatenschutzbeauftragten seien.[13]

1 Andrea_Voßhoff_soll_Bundesdaten schutzbeauftragte_werden_tagesschau.de_-_2013-12-18-15.30.35.html.

2 Auch wenn, wie vorliegend, die Person der/des Datenschutzbeauftragten vom Parlament gewählt wird.

3 Was aber vorliegend auch bedeutet, dass jemand in seinem neuen Amte wachsen kann. O-Ton des Bundesinnenministers: „Eine hervorragende Juristin".

4 Andrea Voßhoff soll Bundesdatenschutz beauftragte werden: http://www.tagesschau.de/inland/datenschutz314.html

5 http://www.heise.de/newsticker/meldung/EU-Datenschutzbeauftragter-bleibt-kommissarisch-bis-zum-Herbst-2098616.html.

6 http://www.heise.de/newsticker/meldung/EU-Datenschutzbeauftragter-bleibt-kommissarisch-bis-zum-Herbst-2098616.html.

7 ABl. C 219 A/1.

8 ABl. C 219 A/3 „Zulassungsbedingungen".

9 Urteil der großen Kammer des Europäischen Gerichtshofes (EuGH) vom 09.03.20107, Az. C-518/07; DuD 2010, 335 ff.; Urteil des Gerichtshofes (Große Kammer) vom 16. Oktober 2012, Az. C-614/10.

10 Siehe dazu Fn. 26 bei Schild, Die völlige Unabhängigkeit der Aufsichtsbehörden aus europarechtlicher Sicht – zugleich Überlegungen, die bestehende Vertragsverletzung im Bereich der Kontrollbehörden nach Art. 28 EG-DS-RiLi der Bundesrepublik Deutschland endlich zu beenden, DuD 2010, S. 549 ff.

11 Zum Wunsche des Ministers nach Änderungsvorschlägen sei der Einfachheit halber auf den Beitrag von Schild, Die völlige Unabhängigkeit der Aufsichtsbehörden aus europarechtlicher Sicht – zugleich Überlegungen, die bestehende Vertragsverletzung im Bereich der Kontrollbehörden nach Art. 28 EG-DS-RiLi der Bundesrepublik Deutschland endlich zu beenden, DuD 2010, S. 549 ff., verwiesen.

12 „Der Datenschutzbeauftragte und sein Stellvertreter nehmen u.a. folgende Aufgaben wahr".

13 Die Frage wurde wohl tatsächlich so gestellt und ist im Lichte von Art. 47 der Charta der Grundrechte, wonach Rechtsschutz von einem „unabhängigen Gericht" zu gewähren ist, durchaus zu hinterfragen. Zumindest ist die Besoldung des Europäischen Datenschutzbeauftragten an die eines Richters am Gerichtshof der Europäischen Union gleichgestellt.

Auszüge aus dem Koalitionsvertrag „Deutschlands Zukunft gestalten“

zwischen CDU, CSU und SPD vom Herbst 2013 für die 18. Legislaturperiode des Deutschen Bundestags zu den Themen Datenschutz und Informationsfreiheit

Vollbeschäftigung, gute Arbeit und soziale Sicherheit, S. 70

Beschäftigtendatenschutz gesetzlich regeln

Die Verhandlungen zur Europäischen Datenschutzgrundverordnung verfolgen wir mit dem Ziel, unser nationales Datenschutzniveau - auch bei der grenzüberschreitenden Datenverarbeitung - zu erhalten und über das Europäische Niveau hinausgehende Standards zu ermöglichen. Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen.

Informantenschutz im Arbeitsverhältnis

Beim Hinweisgeberschutz prüfen wir, ob die internationalen Vorgaben hinreichend umgesetzt sind. …

Zusammenhalt der Gesellschaft, S. 124

Verbraucherschutz

Verbraucher sollen selbstbestimmt entscheiden können. Unser Ziel ist ein verbraucherfreundlicher, transparenter Markt, auf dem sichere und gute Produkte unter fairen und nachhaltigen Bedingungen hergestellt und angeboten werden. Verbraucherpolitik hat auch das Ziel, das Vertrauen zwischen Wirtschaft und Verbrauchern zu stärken. Ungleichgewichte im Markt beseitigen wir, indem wir für Transparenz, Vergleichbarkeit und Möglichkeiten einer effektiven Rechtsdurchsetzung sorgen. Unserer Politik liegt ein differenziertes Verbraucherbild zugrunde. Bedürfnisse, Interessen und Wissen der Verbraucher variieren je nach Markt. Wo Verbraucher sich nicht selbst schützen können oder überfordert sind, muss der Staat Schutz und Vorsorge bieten. Zudem muss er die Verbraucher durch gezielte und umfassende Information, Beratung und Bildung unterstützen. Dies gilt insbesondere für neue Bereiche wie den Finanzmarkt und Digitale Welt. Dafür wollen wir die bestehenden Verbraucherorganisationen mit einer speziellen Marktwächterfunktion „Finanzmarkt“ und „Digitale Welt“ beauftragen.

Zusammenhalt der Gesellschaft, S. 125

Die Stiftung Datenschutz soll in die Stiftung Warentest integriert werden.

Europäisches und internationales Verbraucherrecht

… Bei einem Freihandelsabkommen zwischen der EU und den USA müssen die hohen europäischen Standards u. a. im Verbraucher- und Datenschutz weiter Geltung behalten. …

Zusammenhalt der Gesellschaft, S. 127

Sicherheit, Selbstbestimmung und Transparenz in der digitalen Welt

Wir fördern Innovationen und Techniken, die sicherstellen, dass Profilbildung und darauf basierende Geschäftsmodelle ohne die Erhebung individualisierter personenbezogener Daten auskommen können. Nicht-anonyme Profilbildungen müssen an enge rechtliche Grenzen und die Einwilligung der Verbraucher geknüpft werden. Unternehmen, die Scoringverfahren anwenden, werden verpflichtet, dies der zuständigen Behörde anzuzeigen. Wir werden die Rechtsgrundlage dafür schaffen, dass die Verbraucherverbände datenschutzrechtliche Verstöße abmahnen und Unterlassungsklage erheben können.

Den mobilen Commerce werden wir verbraucherfreundlich ausgestalten, zum Beispiel durch transparente Darstellungsmöglichkeiten auf mobilen Endgeräten und Rückgabemöglichkeiten von Apps. Wir stärken die Rechte von Verbrauchern bei der Nutzung digitaler Güter gegenüber der Marktmacht globaler Anbieter. …

Zusammenhalt der Gesellschaft, S. 139

Erfolgsfaktor der Energiewende ist die Digitalisierung der Energieversorgung. Verkehrsinfrastrukturen werden sowohl im Individualverkehr als auch im öffentlichen Verkehr digitalisiert. Wesentliche Veränderung im Gesundheitswesen ist der Aufbau der Telematikinfrastruktur. Maßgeblicher Faktor der Digitalisierung ist die Globalisierung der Netze und die internationale Arbeitsteilung im Bereich der Informationstechnik. Das weltweite Netz ist ein globales Freiheitsversprechen. Doch spätestens der NSA-Skandal hat die Verletzlichkeit der digitalen Gesellschaft aufgezeigt. IT-Sicherheit wird zu einer wesentlichen Voraussetzung zur Wahrung der Freiheitsrechte. Die gesellschaftlichen Chancen und ökonomischen Poten-

ziale der Digitalisierung dürfen nicht gefährdet werden.

Die Koalition wird für das Handeln aller Ressorts eine digitale Agenda 2014 – 2017 beschließen und ihre Umsetzung gemeinsam mit Wirtschaft, Tarifpartnern, Zivilgesellschaft und Wissenschaft begleiten.

Digitales Wachstumsland Nr. 1 in Europa

Wir wollen die Informations-und Kommunikations-Strategie (IKT-Strategie) für die digitale Wirtschaft weiterentwickeln. Dazu gehören für uns Spitzenforschung im nationalen und europäischen Rahmen, die Entwicklung und Anwendung von digitalen Technologien und optimale Wachstumsbedingungen für Unternehmen aller Branchen. Um den globalen und sicherheitspolitischen Herausforderungen zu begegnen, fördern wir die deutsche und europäische IKT-Industrie, indem wir die Rahmenbedingungen dafür verbessern und Bürokratie abbauen.

Wir wollen Kernbereiche der deutschen Wirtschaft wie Fahrzeug- und Maschinenbau, Logistik und Gesundheitswirtschaft bei der Digitalisierung unterstützen und die Rahmenbedingungen für Unternehmen so ausgestalten, damit diese global wettbewerbsfähig bleiben.

Die Digitalisierung der klassischen Industrie mit dem Zukunftsprojekt Industrie 4.0 werden wir vorantreiben und im nächsten Schritt um intelligente Dienstleistungen („Smart Services“) erweitern, sowie Projekte und Maßnahmen im Bereich der Green IT stärken. Dazu ist es notwendig, Wissen aus der Spitzenforschung in konkrete Anwendungen zu überführen. Mittels Kompetenzzentren, Modellregionen und Pilotprojekten soll der Wissenstransfer in Mittelstand und klassische Industrie initialisiert werden.

Neben dem Zukunftsprojekt Industrie 4.0 werden wir in den Bereichen intelligente Mobilität, Smart Grid, E-Health und Sicherheit Schwerpunkte setzen und damit die Position der deutschen Wirtschaft auf dem Weltmarkt festigen.

Um das zu erreichen, werden Spitzencluster und Verbundprojekte aus- und aufgebaut. Dabei sind ökologische, ökonomische und soziale Nachhaltigkeit maßgebliche Faktoren.

Wir werden Beratungsangebote zur Digitalisierung von bestehenden Wertschöpfungsketten in Industrie und Mittelstand im Hinblick u. a. auf Cloud-Computing und

Zusammenhalt der Gesellschaft, S. 140

Big Data ausbauen. Die Themen IT-Sicherheit und die Abwehr von Wirtschaftsspionage sollen darüber hinaus eine besondere Rolle spielen.

Wir werden die Forschungs- und Innovationsförderung für „Big Data“ auf die Entwicklung von Methoden und Werkzeugen zur Datenanalyse ausrichten, Kompetenzzentren einrichten und disziplinübergreifend strategische Anwendungsprojekte ins Leben rufen. Wir wollen die deutsche Spitzenposition im Bereich des Höchstleistungsrechnens in Abstimmung mit den Ländern und Partnern in Europa weiterhin ausbauen. …

Zusammenhalt der Gesellschaft, S 141

Digitale Bildung und Forschung – gerecht und innovativ

Ein wichtiger Teil der Digitalisierungsstrategie ist es, die Medienkompetenz junger Menschen zu steigern, um sie zu einem sicheren und verantwortungsbewussten Umgang mit dem Internet zu emanzipieren. Wir sehen die Vermittlung von Medien- und Informationskompetenz als zentrale Maßnahme für den Datenschutz und die Sicherheit im Internet für jede einzelne Nutzerin und jeden einzelnen Nutzer. Die bestehenden Programme zur Förderung von Medienkompetenz an Kitas und Schulen werden deshalb evaluiert und ausgebaut. Das Leitbild der „digitalen Selbständigkeit“ rückt somit in den Fokus der Medienkompetenz. Wir befürworten ein „Modellprojekt Freiwilliges Soziales Jahr Digital“, damit junge Menschen ihre technischen Fertigkeiten und Fähigkeiten im Umgang und in der Anwendung von neuen Medien in den Dienst von gemeinnützigen Einrichtungen stellen und diese bei der Umsetzung von digitalen Projekten und der Vermittlung von Medienkompetenz unterstützen. Die Initiative „Ein Netz für Kinder“ wird unterstützt und verbreitert, um in Zusammenarbeit von Politik, Wirtschaft und Institutionen qualitätsvolle, altersgerechte und interessante digitale Angebote für Kinder zu schaffen.

Der Aufbau, der Ausbau und die koordinierte nationale, europäische und internationale Vernetzung von offenen (Forschungs-)Datenbanken, Repositorien und Open-Access-Zeitschriften der Forschungseinrichtungen und der Hochschulen sind im Rahmen eines eigenen Programms zu fördern.

Die Grundlagenforschung zu Internet und digitaler Gesellschaft wird durch gezielte Initiativen zur Programmforschung und durch Bereitstellung entsprechender Mittel gestärkt und verstetigt sowie institutionell gefördert. Ein mit öffentlichen Mitteln finanziertes Internet-Institut, das gleichzeitig als Ausgangspunkt für ein interdisziplinäres Kompetenznetz dient, soll sich mit den technischen und wirtschaftlichen, aber auch den politischen, rechtlichen und ethischen Aspekten des Internets beschäftigen.

Zusammenhalt der Gesellschaft, S. 142

Digitales Leben und Arbeiten – Chancen und Rechte stärken

… Immer mehr Unternehmen nutzen Online-Plattformen, um neue Mitarbeiterinnen und Mitarbeiter zu

gewinnen (E-Recruiting). Hierbei müssen die Grenzen der Privatsphäre eingehalten werden. Eine Umgehung von Privatsphäre-Einstellungen in sozialen Netzwerken oder ähnlichen Plattformen ist nicht zu akzeptieren …

Im Bereich der Gesundheit nutzen wir die Chancen der Digitalisierung und verstärken die Telemedizin, z. B. zur engen Betreuung von Risikopatientinnen und -patienten oder chronisch Kranken. Dabei ist ein Höchstmaß an Datenschutz zu gewährleisten. Wir werden verhindern, dass sensible Patientendaten unkontrolliert an Dritte weitergegeben werden. Bürokratische und rechtliche Hemmnisse in der Telemedizin sollen abgebaut werden, um die Anwendung grundsätzlich zu vereinfachen. Wir wollen den Einsatz und die Entwicklung von E-Care-Systemen in sogenannten Smart-Home-Umgebungen fördern, die älteren, pflegebedürftigen Menschen oder Menschen mit Behinderung die technische Unterstützung bieten, um ihnen den Alltag zu erleichtern. Ein weiterer Fokus liegt auf der Elektronischen Gesundheitskarte (eGK). Die eGK soll ausgebaut werden, um den bürokratischen Aufwand für Patientinnen und Patienten zu verringern und die Kommunikation zu verbessern. Höchste Datenschutzstandards sowie eine sichere Verschlüsselung der Daten sind dabei die Grundvoraussetzung. …

Zusammenhalt der Gesellschaft, S. 143

… Im digitalen Zeitalter hat sich die Art der Kommunikation grundlegend verändert und die Menschen tauschen sich online auf diversen Plattformen aus. Wir sprechen uns gegen einen allgemeinen Klarnamenzwang aus, weil anonyme Kommunikation oft nicht nur sinnvoll, sondern auch notwendig ist. Wir sehen neben den Chancen der Digitalisierung auch die Risiken. So wollen wir Präventions- und Beratungsangebote zu online basiertem Suchtverhalten bundesweit ausbauen und wissenschaftlich begleiten.

In den nächsten vier Jahren können die Weichen gestellt werden, damit Deutschland und Europa eine Führungsrolle bei der konsequenten, sozialverträglichen, vertrauenswürdigen und sicheren Digitalisierung der Gesellschaft und Wirtschaft einnehmen. Mit einer ausgewogenen Digitalisierungspolitik können Zukunftschancen unseres Landes, Potenziale für Demokratie und Teilhabe sowie Innovations- und Wettbewerbsfähig langfristig gesichert werden. Deutschland wird zu einer echten digitalen Gesellschaft.

Moderner Staat, innere Sicherheit und Bürgerrechte, S. 144

5. Moderner Staat, innere Sicherheit und Bürgerrechte

5.1. Freiheit und Sicherheit

Konsequenzen aus den Erkenntnissen des NSU-Untersuchungsausschusses

Der Untersuchungsausschuss des Deutschen Bundestages zum sogenannten „Nationalsozialistischen Untergrund“ (NSU) hat parteiübergreifend zahlreiche Reformvorschläge für die Bereiche Polizei, Justiz und Verfassungsschutz, zur parlamentarischen Kontrolle der Tätigkeit der Nachrichtendienste sowie zur Zukunft der Förderung zivilgesellschaftlichen Engagements gegen Rechtsextremismus, Rassismus und Antisemitismus erarbeitet. Soweit die Bundesebene betroffen ist, machen wir uns diese Empfehlungen zu Eigen und werden sie zügig umsetzen. Soweit die Länder betroffen sind, werden wir im Dialog mit ihnen Wege für die Umsetzung dieser Empfehlungen erarbeiten, etwa bei der einheitlichen Verfahrensführung der Staatsanwaltschaften.

Wir stärken die Zentralstellenfunktion des Bundesamtes für Verfassungsschutz (BfV), bauen dessen Koordinierungskompetenz im Verfassungsschutzverbund aus und verbessern die technische Analysefähigkeit des BfV. Der gegenseitige Austausch von Informationen zwischen Bund und Ländern wird gemeinsame Lagebilder ermöglichen.

Wir wollen eine bessere parlamentarische Kontrolle der Nachrichtendienste. Die Anforderungen an Auswahl und Führung von V-Leuten des Verfassungsschutzes werden wir im Bundesverfassungsschutzgesetz regeln und die parlamentarische Kontrolle ermöglichen. Die Behördenleiter müssen die Einsätze der V-Leute genehmigen. Bund und Länder informieren sich wechselseitig über die eingesetzten V-Leute. …

Moderner Staat, innere Sicherheit und Bürgerrechte, S. 145

Kriminalität und Terrorismus

Prävention …

… Wir wollen unsere Unternehmen vor Wirtschafts- und Konkurrenzspionage aus aller Welt schützen und eine nationale Strategie für den Wirtschaftsschutz erarbeiten. An private Sicherheitsdienstleister stellen wir verbindliche Anforderungen an Seriosität und Zuverlässigkeit.

Zur besseren Bekämpfung von Kinderpornographie im Internet werden wir im
Strafrecht den veralteten Schriftenbegriff zu einem modernen Medienbegriff erweitern. Wir schließen zudem inakzeptable Schutzlücken und beseitigen Wertungswidersprüche im Sexualstrafrecht. Zur Aufklärung von Sexual- und Gewaltverbrechen sollen bei Massen-Gentests auch sogenannte Beinahetreffer verwertet werden können, wenn die Teilnehmer vorab über die Verwertbarkeit zulasten von Verwandten belehrt worden sind. Zum Schutz der Bevölkerung vor höchstgefährlichen, psychisch gestörten Gewalt- und Sexualstraftätern, deren besondere Gefährlichkeit sich erst während der Strafhaft herausstellt, schaffen wir die Möglichkeit der nachträglichen Therapieunterbringung. Die längerfristige Observation

von entlassenen Sicherungsverwahrten stellen wir auf eine gesetzliche Grundlage.

Moderner Staat, innere Sicherheit und Bürgerrechte, S. 146

Effektive Strafverfolgung und wirksame Maßnahmen zur Gefahrenabwehr

… Um eine Alternative zur Freiheitsstrafe und eine Sanktion bei Personen zu schaffen, für die eine Geldstrafe kein fühlbares Übel darstellt, werden wir das Fahrverbot als eigenständige Sanktion im Erwachsenen- und Jugendstrafrecht einführen. Bei Verkehrsdelikten streben wir an, zur Bestimmung der Blutalkoholkonzentration auf körperliche Eingriffe zugunsten moderner Messmethoden zu verzichten. Eine Blutentnahme wird durchgeführt, wenn der Betroffene sie verlangt.

Wir evaluieren die Vorschriften zur Kronzeugenregelung und zur Verständigung im Strafverfahren. Wir prüfen, inwieweit dem öffentlichen Interesse an einem Gerichtsverfahren durch eine erweiterte Saalöffentlichkeit Rechnung getragen werden kann. Im Strafvollzug verbessern wir den Datenaustausch zwischen den beteiligten Einrichtungen und Institutionen.

… Die Vorgaben des Bundesverfassungsgerichts zur Antiterrordatei werden umgesetzt und die Analysefähigkeit der Datei verbessert. Die Vorschriften über die Quellen-Telekommunikationsüberwachung werden wir rechtsstaatlich präzisieren, um unter anderem das Bundeskriminalamt bei seiner Aufgabenerfüllung zu unterstützen.

Moderner Staat, innere Sicherheit und Bürgerrechte, S. 147

Vorratsdatenspeicherung

Wir werden die EU-Richtlinie über den Abruf und die Nutzung von Telekommunikationsverbindungsdaten umsetzen. Dadurch vermeiden wir die Verhängung von Zwangsgeldern durch den EuGH. Dabei soll ein Zugriff auf die gespeicherten Daten nur bei schweren Straftaten und nach Genehmigung durch einen Richter sowie zur Abwehr akuter Gefahren für Leib und Leben erfolgen. Die Speicherung der deutschen Telekommunikationsverbindungsdaten, die abgerufen und genutzt werden sollen, haben die Telekommunikationsunternehmen auf Servern in Deutschland vorzunehmen. Auf EU-Ebene werden wir auf eine Verkürzung der Speicherfrist auf drei Monate hinwirken. Wir werden das Waffenrecht im Hinblick auf die technische Entwicklung und auf seine Praktikabilität hin anpassen. Die Sicherheit der Bürgerinnen und Bürger hat dabei oberste Priorität. Wir streben eine erneute befristete Amnestie an. Zur Erhöhung der öffentlichen Sicherheit werden wir darüber hinaus gemeinsam mit den Ländern schrittweise das nationale Waffenregister weiterentwickeln. Die Kriminal-und Rechtspflegestatistiken machen wir aussagekräftiger. Die Sicherheitsforschung wird besser koordiniert.

Digitale Sicherheit und Datenschutz

Ziel der Koalition ist es, die Balance zwischen Freiheit und Sicherheit auch in der digitalen Welt zu schaffen und zu bewahren.

Cyberkriminalität

Das Strafrecht passen wir – auch durch Abschluss internationaler Abkommen – an das digitale Zeitalter an. Wir schließen Schutzlücken und systematisieren die bisher verstreut geregelten datenbezogenen Strafvorschriften. Wir verbessern den strafrechtlichen Schutz vor Beleidigungen in sozialen Netzwerken und Internetforen (Cybermobbing und Cybergrooming), da die Folgen für die vor einer nahezu unbegrenzten Öffentlichkeit diffamierten Opfer besonders gravierend sind. Cybermobbing und Cybergrooming in sozialen Netzwerken müssen einfacher gemeldet und angezeigt werden können.

Eine zentrale Meldestelle für Phishing und ähnliche Delikte soll die Prävention verbessern und Ermittlungen erleichtern.

IT-Infrastruktur und digitaler Datenschutz

Wir schaffen ein IT-Sicherheitsgesetz mit verbindlichen Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen und der Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle. Dafür setzen wir uns auch auf der EU-Ebene im Rahmen der europäischen Cybersicherheitsstrategie ein.

Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung

Moderner Staat, innere Sicherheit und Bürgerrechte, S. 148

vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.

Wir bauen die Kapazitäten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und auch des Cyber-Abwehrzentrums aus. Wir verbessern die IT-Ausstattung der deutschen Sicherheitsbehörden. Um Bürgerdaten besser zu schützen und zu sichern, werden wir die Bündelung der IT-Netze des Bundes in einer einheitlichen Plattform „Netze des Bundes“ anstreben. IT- und TK-Sicherheit wollen wir zusammenführen.

Die Bundesbehörden werden verpflichtet, zehn Prozent ihrer IT-Budgets für die Sicherheit ihrer Systeme zu verwenden.

Um Vertrauen wieder herzustellen müssen die Standardisierungsgremien transparenter werden. Zudem muss sich Deutschland stärker in diesen und anderen internationalen Gremien beteiligen, besonders solchen der Internetarchitektur und Internet-Governance.

Wir prüfen, inwieweit ein Ausverkauf von nationaler Expertise und Knowhow in Sicherheits-Schlüsseltechnologien verhindert werden kann.

Wir initiieren ein Spitzencluster „IT-Sicherheit und kritische IT-Infrastruktur". Um zu gewährleisten, dass die Nutzerinnen und Nutzer über die Sicherheitsrisiken ausreichend informiert sind, sollen Internetprovider ihren Kunden melden, wenn sie Hinweise auf Schadprogramme oder ähnliches haben. Darüber hinaus streben wir einen sicheren Rechtsrahmen und eine Zertifizierung für Cloud-Infrastrukturen und andere sicherheitsrelevante Systeme und Dienste an.

Zur Wahrung der technologischen Souveränität fördern wir den Einsatz national entwickelter IT-Sicherheitstechnologien bei den Bürgerinnen und Bürgern.

Die Weiterentwicklung und Verbreitung von Chipkartenlesegeräten, Kryptographie, DE-Mail und sicheren Ende-zu-Ende-Verschlüsselungen sowie vertrauenswürdiger Hard- und Software gilt es erheblich auszubauen.

IT-Hersteller und -Diensteanbieter sollen für Datenschutz- und IT-Sicherheitsmängel ihrer Produkte haften.

Wir wollen das vom Bundesverfassungsgericht entwickelte Grundrecht auf Gewähr-leistung der Vertraulichkeit und Integrität informationstechnischer Systeme mit Leben füllen. Die Nutzung von Methoden zur Anonymisierung, Pseudonymisierung und Datensparsamkeit müssen zu verbindlichen Regelwerken werden.

Wir werden den technikgestützten Datenschutz („Privacy by Design") und den Datenschutz durch Voreinstellungen („Privacy by Default") ausbauen.

Moderner Staat, innere Sicherheit und Bürgerrechte, S.149

Um die Grund- und Freiheitsrechte der Bürgerinnen und der Bürger auch in der digitalen Welt zu wahren und die Chancen für die demokratischen Teilhabe der Bevölkerung am weltweiten Kommunikationsnetz zu fördern, setzen wir uns für ein Völkerrecht des Netzes ein, damit die Grundrechte auch in der digitalen Welt gelten. Das Recht auf Privatsphäre, das im Internationalen Pakt für bürgerliche und politische Rechte garantiert ist, ist an die Bedürfnisse des digitalen Zeitalters anzupassen.

EU-Datenschutzgrundverordnung

Die EU-Datenschutzgrundverordnung muss zügig weiter verhandelt und schnell verabschiedet werden, um europaweit ein einheitliches Schutzniveau beim Datenschutz zu garantieren. Die strengen deutschen Standards beim Datenschutz, gerade auch beim Datenaustausch zwischen Bürgern und Behörden, wollen wir bewahren. Europa braucht ein einheitliches Datenschutzrecht für die Wirtschaft, in dem alle Anbieter, die in Europa ihre Dienste anbieten, dem europäischen Datenschutzrecht unterliegen (Marktortprinzip). Die Grundsätze der Zweckbindung, der Datensparsamkeit und -sicherheit, der Einwilligungsvorbehalt, das Recht auf Löschen und das Recht auf Datenportabilität müssen in der Verordnung gewahrt bleiben. Bei den EU-Regelungen zur justiziellen und polizeilichen Zusammenarbeit muss sichergestellt werden, dass das deutsche Datenschutzniveau bei der Übermittlung von Daten an andere EU-Staaten nicht unterlaufen werden darf.

Bei deren Ausgestaltung ist darauf zu achten, dass bestehende Refinanzierungsmöglichkeiten journalistisch-redaktioneller Medien erhalten bleiben und dass das für Presse-und Medienfreiheit unabdingbare Medienprivileg effektiv ausgestaltet wird.

Konsequenzen aus der NSA-Affäre

Wir drängen auf weitere Aufklärung, wie und in welchem Umfang ausländische Nachrichtendienste die Bürgerinnen und Bürger und die deutsche Regierung ausspähen. Um Vertrauen wieder herzustellen, werden wir ein rechtlich verbindliches Abkommen zum Schutz vor Spionage verhandeln. Damit sollen die Bürgerinnen und Bürger, die Regierung und die Wirtschaft vor schrankenloser Ausspähung geschützt werden. Wir stärken die Spionageabwehr. Unsere Kommunikation und Kommunikationsinfrastruktur muss sicherer werden. Dafür verpflichten wir die europäischen Telekommunikationsanbieter, ihre Kommunikationsverbindungen mindestens in der EU zu verschlüsseln und stellen sicher, dass europäische Telekommunikationsanbieter ihre Daten nicht an ausländische Nachrichtendienste weiterleiten dürfen. Die Koalition tritt für die europaweite Einführung einer Meldepflicht für Unternehmen an die EU ein, die Daten ihrer Kundinnen und Kunden ohne deren Einwilligung an Behörden in Drittstaaten übermitteln. Wir werden zudem in der EU auf Nachverhandlungen der Safe-Harbor und Swift-Abkommen drängen. …

Moderner Staat, innere Sicherheit und Bürgerrechte, S.149

Bürgerbeteiligung

Parlament, Regierung und Verwaltung werden die Möglichkeiten der Digitalisierung intensiv nutzen und die interaktive Kommunikation mit den Bürgerinnen und Bürgern sowie der Wirtschaft auf barrierefreien

Websites ausbauen. Wir wollen die Potenziale der Digitalisierung zur Stärkung der Demokratie nutzen. Wir wollen die Informationen über politische Entscheidungen quantitativ und qualitativ verbessern und die Beteiligungsmöglichkeiten für die Menschen an der politischen Willensbildung ausbauen. Gerade im Vorfeld von Entscheidungen ist früh, offen, umfassend und verständlich zu informieren. Deutschland wird im Rahmen der „Digitalen Agenda" der EU-Kommission einen „Digital Champion" benennen. …

Moderner Staat, innere Sicherheit und Bürgerrechte, S. 152

Transparenter Staat

Die digitale Berichterstattung über den Bundestag und seine Sitzungen sowie über öffentliche Ausschusssitzungen und Anhörungen (z. B. in Streams) wollen wir ausbauen. So bald wie möglich werden wir Bekanntmachungen wie beispielsweise Drucksachen und Protokolle in Open Data tauglichen Formaten unter freien Lizenzbedingungen bereitstellen. …

Moderne Verwaltung

Wir wollen ein bürgerfreundliches „digitales Deutschland". Ein Programm „Digitale Verwaltung 2020" für verbindliche Standards zur flächendeckenden Digitalisierung der Verwaltung soll dazu auf den Weg gebracht werden. Bei den Beschaffungen des Bundes werden wir die Prozesse standardisieren und nach Möglichkeit digitalisieren.

Durch E-Government ergeben sich umfassende Dienstleistungen für die Bürgerinnen und Bürger und für die Wirtschaft, die die Erledigung von Formalia wie Behördengängen wesentlich erleichtern können. Zahlreiche gute und erfolgreiche E-Government-Projekte zeigen, dass es innovative technische Lösungen in Deutschland gibt, die allerdings noch nicht flächendeckend und koordiniert umgesetzt sind.

Der Bund wird den Ländern vorschlagen, die Programme des E-Governments unter Verantwortung des IT-Planungsrates zu konsolidieren und zu koordinieren. Dabei sind Technologien nach Möglichkeit langfristig so zu planen, dass keine Abhängigkeiten zu intransparenten Protokollen, Software, Hardware oder Herstellern entstehen.

Bei der Anschaffung von IT-Technologie durch die öffentliche Hand müssen im Rahmen des Wirtschaftlichkeitsprinzips Innovationspotenziale und Nachhaltigkeit als mitentscheidende Kriterien bedacht werden. Bei Ausschreibungen sollen Sicherheitsstandards vorgegeben und wenn möglich Open-Source-Lösungen erwogen werden.

Voraussetzung für die Akzeptanz elektronischer Behördendienste sind Datenschutz und Sicherheit der Kommunikation und Angebote. Die Identifizierungsfunktion des neuen Personalausweises und die Nutzung von Ende-zu-Ende-Verschlüsselungen sind grundsätzlich anzuwenden.

Moderner Staat, innere Sicherheit und Bürgerrechte, S. 153

… Die Bürgerinnen und Bürger sollen auf Wunsch die Möglichkeit haben, einen einheitlichen Stammdaten-Account, ein sogenanntes Bürgerkonto zu verwenden, um die Kommunikation mit der Verwaltung zusätzlich zu vereinfachen. Zur elektronischen Identifizierung soll der neue elektronische Personalausweis genutzt werden. Das Bürgerkonto kann zum digitalen Dokumentenpostfach erweitert werden.

Eine Systematisierung der bislang nebeneinander stehenden Rechtsregelungen zum Internet (Internetgesetzbuch) wird geprüft und in diesem Zusammenhang das Leistungsschutzrecht hinsichtlich der Erreichung seiner Ziele evaluiert.

Erste Open-Data-Projekte in Deutschland zeigen das Potential offener Daten. Die Bundesverwaltung muss auf der Basis eines Gesetzes mit allen ihren Behörden Vorreiter für die Bereitstellung offener Daten in einheitlichen maschinenlesbaren Formaten und unter freien Lizenzbedingungen sein. Wir wollen für Bund, Länder und Kommunen ein Open-Data-Portal bereitstellen. Die Koalition strebt einen Beitritt Deutschlands zur internationalen Initiative Open Government Partnership an. …

Starkes Europa, S. 162

Die Rolle, die Europa im 21. Jahrhundert spielen wird, hängt auch entscheidend davon ab, ob es uns gelingt, im Bereich der digitalen Welt Anschluss zu halten, europäische Standards zu setzen und damit unser europäisches Gesellschaftsmodell zu bewahren. Deshalb treten wir für eine umfassende europäische digitale Agenda ein, die Verbraucherschutz, Datenschutz, Innovation, Netz und Informationssicherheit zusammen bringen.

Nötig ist zudem ein neuer internationaler Rechtsrahmen für den Umgang mit unseren Daten. Unser Ziel ist eine internationale Konvention für den weltweiten Schutz der Freiheit und der persönlichen Integrität im Internet. Die derzeit laufende Verbesserung der europäischen Datenschutzbestimmungen muss entschlossen vorangetrieben werden. Auf dieser Grundlage wollen wir auch das Datenschutzabkommen mit den USA zügig verhandeln. …



Russia 1984

Russlands Gesetzgeber hat in den letzten Monaten offen angekündigt, eine prinzipiell vollständige Überwachung der Telekommunikation aller seiner Bürger und Gäste einzuführen. Der russische Inlandgeheimdienst soll pauschale Zugriffsrechte auf diese Daten erhalten. Ein Richter-Vorbehalt ist nicht vorgesehen.

Diese Pläne erinnern an totalitäre Fantasien und stehen dem Skandal, der sich angesichts der Snowden-Dokumente rund um die US-Geheimdienste samt aller besser oder schlechter gestellten verbündeten und kooperierenden Spionagedienste anderer Länder offenbart, um nichts nach.

Nur, dass sich so gut wie niemand über diese völlig unversteckt angekündigte Totalüberwachung aufregt. Warum sich die allermeisten der in Deutschland in Verantwortung stehenden Politiker wohl einer Kritik daran enthalten …

Wir haben dem russischen Botschafter in Berlin einen Offenen Brief geschrieben, der am 14.1.2014 per Einschreiben mit Rückschein versendet worden ist:

Protestnote gegen die offen angekündigte Vollüberwachung russischer Telekommunikation, veröffentlicht am 16.01.2014 von freiheitsfoo

Sehr geehrter Herr Grinin,

wir schreiben Ihnen als Initiative „freiheitsfoo“, weil uns einige Meldungen der letzten Monate beunruhigen. Diesen Meldungen zufolge:

- werden in Russland alle IP- und Telefonnummern sowie E-Mail-Adressen kontrolliert und Daten aus sozialen Netzwerken, Internettelefonaten und Chats abgegriffen,
- werden diese Daten, die bereits seit 2008 bei den Telekommunikations-Anbietern vorgehalten werden müssen, ab dem 1.7.2014 unmittelbar in einem staatlichen Rechnersystem namens „Sorm“ zusammengetragen und dort verarbeitet,
- erhält der russische Inlandsgeheimdienst FSB unbeschränkten Zugriff auf diese Datenbank,
- liegt dem russischen Parlament ein Gesetzentwurf vor, wonach der FSB uneingeschränkt soziale Netzwerke nutzen und infiltrieren darf,
- sollen während der Olympischen Winterspiele 2014 in Sotschi alle Besucher und Zuschauer (und selbstverständlich auch die Sportler) vollständig überwacht werden: Jedes Gespräch und jeder Datenverkehr, also jede E-Mail, jegliche Tätigkeit in sozialen Netzwerken oder in Chats sollen abgefangen und belauscht werden und/oder mittels Deep Packet Inspektion überwacht werden.

Diese geplanten und angekündigten Maßnahmen zur Totalerfassung sämtlicher Kommunikation mittels des Internets widersprechen dem von Russland am 23.3.1973 ratifizierten Internationalen Pakt über bürgerliche und politische Rechte, darin insbesondere:

- dem Recht auf Schutz vor willkürlichen Eingriffen in sein Privatleben und in seinen Schriftverkehr (Artikel 17.1),
- dem Recht auf Gedanken- und Gewissensfreiheit (Artikel 18.1),
- dem Recht auf Schutz vor Zwängen oder Einschränkungen im Zusammenhang mit der Religionsfreiheit (Artikel 18.2),
- dem Recht auf unbehinderte Meinungsfreiheit (Artikel 19.1),
- dem Recht auf freie Meinungsäußerung inklusive des Rechts, „ohne Rücksicht auf Staatsgrenzen Informationen und Gedankengut jeder Art in Wort, Schrift oder Druck, durch Kunstwerke oder andere Mittel eigener Wahl sich zu beschaffen, zu empfangen und weiterzugeben“ (Artikel 19.2),
- dem Recht, sich frei mit anderen zusammenzuschließen (Artikel 22.1),
- dem Recht, an der Gestaltung der öffentlichen Angelegenheiten unmittelbar teilzunehmen (Artikel 25).

Diese Überwachungsvorhaben widersprechen aber weiterhin auch dem von Russland am 16.10.1973 ratifizierten Internationalen Pakt über wirtschaftliche, soziale und kulturelle Rechte, darin:

- dem Recht auf Berufsfreiheit (Artikel 6.1),
- dem Recht auf Bildung (Artikel 13.1),
- dem Recht auf Teilnahme am kulturellen Leben (Artikel 15.1),
- dem Recht auf Teilhabe am wissenschaftlichen Fortschritt und seiner Anwendungen (Artikel 15.2),
- dem Urheberrecht (Artikel 15.3),
- dem Recht auf Freiheit der Forschung (Artikel 15.4).

Die seitens der für die beschriebenen Überwachungsmaßnahmen Verantwortlichen vorgebrachten Beruhigungen, dass niemand etwas zu befürchten habe, der nur „anständige und normale“ Internetseiten aufrufe (Zitat des Abgeordneten des russischen Parlaments, Alexander Chinschtejn), laufen sachlich ins Leere, da diese Eingriffsgrenze zum einen einen äußerst weiten und vor allem unscharfen Eingriffstatbestand beschreibt, vor allem aber weil zum zweiten bereits die Anwendung der schon jetzt praktizierten Kommunikations-Erfassungs- und Speicherungsmaßnahmen bei den Providern zu einer unakzeptablen und unverhältnismäßigen Einschränkung grundlegender Menschen- und Freiheitsrechte führt.

Die für den 1.7.2014 angekündigten Erweiterungen des Zugriffs auf diese Daten und deren Verarbeitung durch Geheimdienste verstärkt diese aus unserer Sicht unzulässigen Beschneidungen noch um ein Vielfaches.
Genau so wie wir die unserer Meinung nach illegalen und im letzten halben Jahr offenbar gewordenen Überwachungsmaßnahmen vieler internationaler Spionagedienste verurteilen (auch die der deutschen Dienste!), wenden wir uns nun also hiermit an Sie als den offiziellen Vertreter der Russischen Föderation in Deutschland:

Sehr geehrter Herr Grinin, die oben beschriebenen Überwachungsmaßnahmen Russlands widersprechen fundamentalen Menschen- und Bürgerrechten. Sie greifen die freiheitliche Entwicklung der russischen Gesellschaft an, sie unterdrücken die Menschen in Russland und nicht nur in Russland.

Bitte, Herr Grinin, setzen Sie sich für eine Abkehr der russischen Politik von diesem Überwachungswahn ein. Bitte initiieren und unterstützen Sie internationale Anstrengungen zur weltweiten Abwendung des Trends der Verselbständigung von staatlichen Geheimdiensten und privatwirtschaftlicher Überwachung.

Strikte Datensparsamkeit und ein bewusster staatlicher Informationsverzicht als Ausdruck eines modernen freiheitlich-demokratischen Selbstverständnisses sollten die Zielpunkte einer Idee von einer Welt sein, in der möglichst alle Menschen friedlich leben und sich frei entfalten können.

Wir würden uns sehr freuen, von Ihnen eine Stellungnahme zu unserer Intervention zu erhalten.

Diesen Brief verstehen wir als offenen Brief und selbstverständlich werden wir Ihre Stellungnahme ebenso ungekürzt im Netz der interessierten Öffentlichkeit zur Verfügung stellen.

Mit vielen guten Grüßen,
die Menschen von freiheitsfoo.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Andrea Voßhoff neue BfDI

Am 06.01.2014 wurde Andrea Voßhoff zur 6. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ernannt. Sie ist damit die erste Frau in diesem seit 1978 bestehenden Amt. Die Ernennungsurkunde wurde von Bundesinnenminister Dr. Thomas de Maizière (CDU) überreicht. Die 55-jährige Juristin Andrea Voßhoff war 14 Jahre lang Mitglied des Deutschen Bundestags und zuletzt seit 2010 rechtspolitische Sprecherin der CDU/CSU-Bundestagsfraktion. Voßhoff ist in Niedersachsen geboren und hat in Münster und in Lausanne Jura studiert. Sie hat als Rechtsanwältin sowie in einem Notarbüro gearbeitet. Seit 1986 ist sie CDU-Mitglied. Seit Anfang der 90er Jahre lebt Voßhoff im brandenburgischen Rathenow.

Das Amt des Bundesbeauftragten für den Datenschutz wurde Anfang 2006 um das Amt des Bundesbeauftragten für die Informationsfreiheit ergänzt. In der Dienststelle arbeiten 85 Beschäftigte in Bonn und Berlin. Die Bundesbeauftragte berät und kontrolliert Bundesbehörden, andere öffentliche Stellen des Bundes sowie Telekommunikations- und Postdienstunternehmen. Zudem berät und kontrolliert sie die Durchführung von Sicherheitsüberprüfungen nach dem Sicherheitsüberprüfungsgesetz des Bundes, auch soweit sie private Unternehmen betreffen. Die BfDI ist Mitglied der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und vertritt Deutschland in der Artikel-29-Gruppe, einer europäischen Arbeitsgruppe der Datenschutzbeauftragten der EU-Mitgliedstaaten, sowie in den europäischen und internationalen Konferenzen der Datenschutz- und Informationsfreiheitsbeauftragten. Ferner wirkt sie in den Gemeinsamen Datenschutz-Kontrollgremien für Europol und das Schengener Informationssystem mit.

Keine Übergangsbesetzung

Der Wahl von Voßhoff war ein seltsames Verhalten des damaligen Bundesinnenministers Hans-Peter Friedrich (CSU) vorausgegangen: Der 17.12.2013 war nicht nur der Tag der Wiederwahl von Angela Merkel als Bundeskanzlerin, sondern auch der letzte Tag der 10jährigen Amtszeit von Peter Schaar als Datenschutzbeauftragter des Bundes. Es wäre nun üblich gewesen, Schaar aufzufordern, bis zur Übernahme durch eine Stellvertreterin weiterhin seine Funktion wahrzunehmen. Friedrich beschloss aber, dass am 17.12. Schluss sein soll; die Überreichung der „Dankesurkunde“ im kleinen Kreise überließ er seiner Staatssekretärin Cornelia Rogall-Grothe.

Dies hatte den ärgerlichen Effekt, dass durch die Vakanz viele Funktionen des BfDI überhaupt nicht mehr wahrgenommen werden konnten. Dies mag über die Feiertage faktisch nicht gravierend gewesen sein, muss aber wohl als Symbol verstanden werden, welchen Stellenwert Friedrich dem Amt des BfDI beimaß - in einer Zeit von Geheimdienst-Abhör- und Spionageaffären. In einer ähnlichen Situation hatte der damalige SPD-Innenminister Otto Schily Schaars Vorgänger Joachim Jacob gebeten, bis zur Wahl des Nachfolgers geschäftsführend im Amt zu bleiben.

Kurz vor seinem Amtsende hatte Peter Schaar die CDU/CSU und SPD aufgefordert, in den Koalitionsverhandlungen eine unabhängigere Stellung des Amtes zu verabreden. Es verstoße gegen europäisches Recht, dass der Datenschutz ans Innenministerium angedockt ist. Bisher sieht das Bundesdatenschutzgesetz vor, dass die Bundesregierung einen Vorschlag macht; die Wahl erfolgt durch den Bundestag. Die Vereidigung erfolgt durch den Innenminister. Die Personalverwaltung erfolgt durch das Bundesinnenministerium: „Ein Ministerium, das sich in erster Linie als Sicherheitsministerium definiert, ist sicherlich nicht der beste Ort für das Thema Datenschutz.“ Sinnvoller sei die Praxis anderer europäischer Staaten oder vieler Bundesländer, das Amt an das Parlament anzubinden. Außerdem kritisierte Schaar die Bundesregierung, welche die NSA-Affäre vorschnell für beendet erklärt hatte. Von Innenminister sei er deshalb „schon arg enttäuscht“: „Das lückenlose Überwachen von Kommunikation, wie es von den Amerikanern offenbar betrieben wird, ist nicht mit unserem Verfassungsverständnis vereinbar. Da müsste der Verfassungsminister klare Worte sprechen. Die habe ich bisher nicht vernommen.“

Kritik an der Personalbesetzung

Der Vorschlag, Voßhoff zur BfDI zu machen, stieß unter DatenschützerInnen auf wenig Begeisterung, nicht nur bei der DVD (siehe S. 16). Die Rechtspolitikerin hatte sich in der Vergangenheit weder durch Datenschutzkenntnisse noch durch ein entsprechendes Engagement profiliert. So meinte der renommierte Datenschützer der ersten Stunde und Jura-Professor Spiros Simitis: „Datenschutzbeauftragte müssen keine Juristen sein. Aber sie müssen die Grundhaltung haben, dass jede staatliche Verarbeitung privater Daten die Ausnahme sein soll, nicht die Regel.“ Voßhoff hatte sich bisher dadurch profiliert, dass sie insbesondere Sabine Leutheusser-Schnarrenberger als Justizministerin immer wieder wegen ihres Datenschutzengagements triezte und zur Zustimmung zu mehr Datensammelei aufforderte, etwa zur Vorratsdatenspeicherung, die zur Verbrechenbekämpfung „dringend notwendig“ sei, so die neue BfDI im Jahre 2011. Das sei allen klar, „die von der Materie etwas

verstehen". Der Bayerische Rundfunk fasst ihre Positionen prägnant zusammen: „Die vom Bundesverfassungsgericht gestoppte Vorratsdatenspeicherung: Andrea Voßhoff war dafür. Die Internetsperren: Voßhoff war dafür. Die Onlinedurchsuchung, bei der mit einem speziellen Programm die Computernutzung von Verdächtigen aufgezeichnet wird: Voßhoff stimmte dafür. Das umstrittene und letztlich gekippte Acta-Abkommen: Voßhoff verteidigte es." Peter Schaar hatte all diese Initiativen abgelehnt.

„Meine Grundposition ist, dass eine datenschutzkonforme Vorratsdatenspeicherung ein wirksames Instrument der Kriminalitätsbekämpfung sein kann." Ihre pragmatische Haltung zeigte Voßhoff auch bei der NSA-Affäre. Sie war mit ihrer Partei und ihrer Fraktion, die sich in Sachen digitalen Grundrechtsschutz nicht mit Ruhm bekleckerten, immer auf Linie und zumeist auf Konfliktkurs zur Position der SPD.

Entsprechend besorgt äußerten sich Mitglieder der Opposition über Voßhoff. Jan Korte, der Vizevorsitzende der Linksfraktion, meinte, es sei fraglich, ob ihre Besetzung das richtige Zeichen sei. Die Linke wollte denn auch die Wahl verhindern und mit einer überfraktionellen Kommission nach einem neuen Kandidaten suchen, scheiterte mit diesem Vorhaben jedoch. Jan Philipp Albrecht, Innenexperte der Grünen im EU-Parlament, fand, dass ihre Berufung der „Abschaffung" des Amtes gleichkommt. Konstantin von Notz, innenpolitischer Sprecher der Grünen im Bundestag, nannte die Benennung eine „merkwürdig anmutende Personalentscheidung". Für ihn sei die Personalie Teil des Versuches der Union, „den Grundrechtsschutz der Bürgerinnen und Bürger auszuhöhlen".

Die Bürgerrechtler vom Verein Digitalcourage kritisierten „eine Personalentscheidung, die irritiert, denn Andrea Voßhoff hat bisher keinerlei Profil im Thema Datenschutz". „Mit dieser Personalentscheidung demonstriert die CDU/CSU ihren Unwillen, den Spähskandal ernst zu nehmen", so Rena Tangens von Digitalcourage. Gerade bei einer Großen Koalition brauche es niemanden, der Regierungsentscheidungen abnicke, sondern eine wirksame Kontrollinstanz für den Datenschutz.

„Neue Akzente"

Unionsfraktionsgeschäftsführer Michael Grosse-Brömer (CDU) verteidigte die Personalentscheidung und bezeichnete Voßhoff als geschätzte Juristin und „gute und richtige Kandidatin" für das Amt. Voßhoff selbst sagt noch nichts zu ihren Plänen. Es sei eine große Herausforderung, den Bürgerdatenschutz im Zeitalter des globalen Netzes zu schützen und vor allem anzupassen, sagte sie nach ihrer Wahl im Bundestag, „auch wenn ich vielleicht in Zukunft den ein oder anderen Akzent anders setze". Wie diese Akzente aussehen könnten, wollte sie jedoch nicht erklären. Die weltweite Überwachung durch die NSA hält sie für ein Problem, sie wolle sich um internationale Lösungen bemühen.

Hintergründe

Die Personalie Voßhoff geht auf einen Deal zwischen Union und SPD bei den Koalitionsgesprächen zurück. Dafür, dass die SPD den Wehrbeauftragten benennen darf, bekam die Union das Auswahlrecht für die BfDI. Die Amtszeit des Wehrbeauftragten Hellmut Könighaus endet erst 2015. Ein SPD-Innenpolitiker beklagte daher: „Es war ein Fehler, auf dieses Amt zu verzichten. Wir können nicht im Wahlkampf die Union beim Thema NSA vor uns hertreiben, um ihr nach der Wahl dieses Bürgerrechtsthema zu schenken."

Voßhoff hatte den Wiedereinzug in den Bundestag verpasst, weil sie in ihrem Wahlkreis in Brandenburg an der Havel durch den Sozialdemokraten Frank-Walter Steinmeier hauchdünn geschlagen wurde. Offensichtlich sah sich die CDU in der Pflicht, der verdienten Parteifrau ein neues Amt zu beschaffen (PE BfDI 06.01.2014, Andrea Voßhoff als Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ernannt; Biermann/Jacobsen, Eine Datenschutzbeauftragte, die Daten nicht schützen will, www.zeit.de 19.12.2013; Braun/Hollenstein, Eine Nachfolgerin für Peter Schaar, SZ 17.12.2013, 6; Kandidaten für den Datenschutz, SZ 13.12.2013, 7; Amann, Ohne Herzblut, Der Spiegel 52/2013; Sindler/Schmid, „Es gibt Opfer", Der Spiegel 45/2013; Braun, Stumm geschaltet, SZ 27.11.2013, 6).

Bund

Kontodatenanfragen steigen weiter

Die Zahl der Kontendatenabfragen durch Finanzämter und Sozialbehörden ist im Jahr 2013 weiter stark gestiegen. Der Bundesdatenschutzbeauftragte Peter Schaar teilte mit, dass es bis Ende September bereits 102.416 Kontenabrufe gab. Im gesamten Jahr 2012 waren es noch 72.578 (vgl. DANA 1/2013, 17). Dies ist ein Anstieg von mehr als 40%. Schaar forderte, dass die sogenannten Kontoabrufersuchen „auf das unbedingt erforderliche Maß" zurückgeführt werden. Deutsche Behörden können seit 2002 bestimmte Kontodaten beim Bundeszentralamt für Steuern abfragen – etwa um Steuerhinterziehungen und den Sozialleistungsmissbrauch aufzudecken. Zudem sollen dadurch Finanzströme des internationalen Terrorismus aufgedeckt werden können. Abgefragt werden dürfen unter anderem Namen des Kontoinhabers und die Kontonummer, nicht aber Kontostände und Kontobewegungen. Schaar kritisierte: „Das Argument des Kampfs gegen den Terrorismus diente – wie wir jetzt wissen – als eine Art Türöffner zu Kontodaten." Bei den Abfragen fehlten oft die konkreten Begründungen, auch würden die Betroffenen nicht wie vorgeschrieben benachrichtigt (Schaar kritisiert steigende Anzahl behördlicher Kontoabfragen, www.zeit.de 26.11.2013).

Bund

Bundesinnenministerium verletzt Mitarbeiterdatenschutz

Das Bundesinnenministerium (BMI) bestätigte am 16.12.2013, dass es dort zu Datenschutzverletzungen beim Umgang mit personenbezogenen Mitarbeiterdaten gekommen ist. Anders als vom Ministerium zugegeben, soll es sich jedoch nicht um einen „Einzelfall", sondern gemäß Presseangaben um Dutzende Fälle gehandelt haben, nicht nur innerhalb des BMI, sondern auch beim elektronischen Postverkehr mit nachgeordneten Behörden wie zum

Beispiel dem Bundesverwaltungsamt (BVA). Nach ministeriumsinternen Angaben kam es zum Beispiel bei der Weitergabe von Bewerbungsunterlagen, die auch personenbezogene Daten enthielten, „in mindestens Dutzenden von Fällen" zu Verletzungen des Datenschutzes seitens des BMI. Die „Welt" hatte berichtet, dass „im Zuge der Umstellung auf die elektronische Akte ärztliche Gutachten eingescannt, elektronisch veraktet und per Mail weitergeleitet" worden sind.

In mehreren internen Beschwerdeschreiben, die an den Personalrat, den Datenschutzbeauftragten des BMI und die Leitung des Hauses gerichtet waren, heißt es: „Diese Unterlagen sind einem unüberschaubaren Personenkreis zugänglich." Dies sei weder mit der Dienstvereinbarung zur Nutzung der elektronischen Akte noch mit der einschlägigen Hausanordnung im BMI vereinbar. Es müsse davon ausgegangen werden, „dass hier systematisch gegen das Datenschutzgesetz verstoßen wird." Darüber hinaus komme es offenbar seit Jahren zu schweren Datenschutzverstößen im Zusammenhang mit Bewerbungsunterlagen von Personen außerhalb des Ministeriums. Deren Unterlagen wurden – inklusive personenbezogener Daten – ebenfalls in dem elektronischen Aktensystem des BMI erfasst und im Haus per E-Mail verschickt.

Zunächst hatte ein Sprecher auf Anfrage erklärt: „Der ‚Welt' vorliegende Informationen, wonach angeblich im elektronischen Aktensystem des Bundesinnenministeriums personenbezogene Daten von Mitarbeitern – unter anderem auch ärztliche Gutachten – systematisch eingescannt, digital gespeichert und per elektronischer Hauspost (E-Mail) in den hausinternen Verkehr gebracht würden, sind falsch." Dies wurde später korrigiert: „In einem Einzelfall seien ärztliche Informationen zu einer Mitarbeiterin" aufgrund eines „Büroversehens" nicht wie vorgeschrieben unkenntlich gemacht worden. Dabei soll es sich jedoch nicht um ein ärztliches Gutachten mit Angaben zum Gesundheitszustand gehandelt haben (BMI gibt „Büroversagen" bei Mitarbeiterdaten zu, Clauß, www.welt.de 16.12.2013).

Bund

Polizei-Fahndung über soziale Netzwerke naht

Die Innenminister des Bundes und der Länder sprachen sich auf ihrer Konferenz im Dezember erneut für die Fahndung mittels Facebook und anderer sozialer Netzwerke aus. Die Bund-Länder-Projektgruppe „Öffentlichkeitsfahndung in sozialen Netzwerken" hatte zuvor ihren Ergebnisbericht vorgestellt. In ihrem Abschlussbericht schreibt die Innenminister-Konferenz, dass sie die Fahndung in sozialen Netzwerken für grundsätzlich zulässig hält. Sie begrüßt, dass sich die Justizministerkonferenz derzeit mit einer Anpassung relevanter Richtlinien befasst.

Einige Tage vor der Konferenz hatte Hamburgs Innensenator Michael Neumann (SPD) im Gespräch mit der Neuen Osnabrücker Zeitung (NOZ) angekündigt, dass er seinen Kollegen bei der Konferenz empfehlen wolle, den Weg für die Facebook-Fahndung freizumachen. Neumann stellte der Konferenz die Ergebnisse der Bund-Länder-Projektgruppe als Berichterstatter vor. Die Nutzung der Netzwerke werde „…die Erfolgsaussichten der Fahndung der Polizei deutlich verbessern.", sagte Neumann der NOZ. Gerade junge Menschen seien vor allem über das Internet zu erreichen. Der Datenschutz müsse jedoch gewahrt bleiben.

Auch auf der Justizministerkonferenz in Berlin im November wurde einstimmig beschlossen, das Thema stärker in den Blick zu nehmen. Der Strafrechtsausschuss hatte Empfehlungen zur Änderung der geltenden Gesetze abgegeben. Die Strafprozessordnung erlaubt die Öffentlichkeitsfahndung bei einer „Straftat von erheblicher Bedeutung". Im Anhang gibt es die Richtlinien für das Strafverfahren und darin das Kapitel über „die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung". Dort heißt es: „Private Internetanbieter sollen grundsätzlich nicht eingeschaltet werden." Suchaufrufe dürfen demnach grundsätzlich nur auf Polizei-Seiten stehen. Diese Richtlinien will der Strafrechtsausschuss nun gemäß seiner Empfehlungen ändern. Die Konferenz glaubt, dass diese Empfehlungen den datenschutzrechtlichen und rechtsstaatlichen Grundsätzen gleichermaßen genügen. Der Strafrechtsausschuss soll vor einer Umsetzung die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beteiligen.

Bislang kommt Facebook in Deutschland als Fahndungshilfe nur vereinzelt zum Einsatz. Neben Niedersachsen fahnden Hessen und Mecklenburg-Vorpommern in dem sozialen Netzwerk, ebenso die Beamten des Bundeskriminalamtes.

(Vensky, Die Fallstricke der Facebook-Fahndung, www.zeit.de 09. Juli 2012; Fisser, Hamburg macht sich für Facebook-Fahndung stark, www.noz.de 02.12.2013; Beschlussniederschrift 84. JMK, TOP II.2 Öffentlichkeitsfahndung in Facebook und anderen sozialen Netzwerken Beschlussniederschrift 198. IMK, Az. VB 2.2, TOP 16: Soziale Netzwerke Öffentlichkeitsfahndung;)

Bayern

Allianz will Datenverarbeitung an US-Konzern outsourcen

Der Allianz-Versicherungskonzern will seine Rechenzentren outsourcen. Gemäß Presseberichten soll der Zuschlag an den US-amerikanischen IT-Konzern IBM gehen, mit dem „exklusive Verhandlungen" begonnen wurden, wie eine Sprecherin der Allianz in München bestätigte: „Wir wollen unsere derzeit mehr als 140 Rechenzentren weltweit in sechs regionalen Standorten zusammenführen. Dazu will der wohl finanzstärkste Versicherungskonzern der Welt die Bereiche Technologie und Rechenzentren in „einem einheitlichen IT-Infrastrukturbetrieb" bündeln. Hierfür soll die in der Rechtsform einer Europäischen Aktiengesellschaft (SE) geführte Allianz SE „eine langfristige globale Partnerschaft" eingehen. Der Partner soll über große Erfahrungen beim Aufbau und Betrieb globaler IT-Strukturen verfügen. Die Verhandlungen sollen noch im Jahr 2013 abgeschlossen werden.

Datenschützer in Deutschland sorgen sich um die Sicherheit der hochsensiblen Informationen, die Rückschlüsse auf die

Finanzen der Allianz-KundInnen zulassen – und warnen vor Spähern etwa des US-Geheimdienstes NSA. Es sei riskant und unverantwortlich, die Daten von 78 Millionen KundInnen weltweit einem US-Konzern anzuvertrauen. Dies könne nach der augenblicklichen Rechtslage möglicherweise sogar unzulässig sein. Die Verarbeitung von deutschen Kundendaten in einer sogenannten Cloud ist einem deutschen Unternehmen grundsätzlich verboten, wenn die IT-Wolke mit Rechenzentren in Ländern verbunden ist, in denen kein effektiver Datenschutz besteht.

Ob konzerninterne Regeln einen Zugriff von ausländischen Behörden ausschließen, ist nicht bekannt. Geheimdienste wie die NSA beschaffen sich bei Bedarf Zugang zu sensiblen Versicherungsdaten, die auch für die US-Steuerbehörden interessant sind. Solche Verletzungen der Vertragsvertraulichkeit können bei einer Verarbeitung durch ein US-Unternehmen derzeit nicht ausgeschlossen werden.

Der in mehr als 70 Ländern tätige Versicherungsriese steht trotzdem zu seinem Geschäftsmodell, mit dem 560 Stellen abgebaut und dadurch Kosten gespart werden sollen, so eine Sprecherin: „Die Allianz wird die Gesamtverantwortung sowie das Design und die Datenhoheit behalten. IBM liefere lediglich „operative Services". Dem Allianz-Vorstand sei der Schutz der Daten ihrer KundInnen, Geschäftspartner und Mitarbeitenden „wichtig" (Pfeiffer, Allianz: Kundendaten in die USA, taz 26.11.2013; Pfeiffer, Allianz gibt Kundendaten ab, http://www.taz.de/Zweifel-an-IT-Sicherheit/!128191/).

Bayern

Einpark-Kamera zeigt Porno

Als ein Fahrer eines Kleinlasters in der Nürnberger Innenstadt parken wollte, hatte er hierfür eine Rückfahrkamera eingeschaltet, mit dem das Einparken erleichtert wird, indem diese den Bereich hinter dem Auto filmt. Die Kamera in dem Kleinlaster wechselte jedoch unerwartet das Programm und zeigte einen Pornofilm. Der Lasterfahrer verständigte daraufhin die Polizei, die feststellte, dass sowohl die Rückfahrkamera wie auch die drahtlose Überwachungskamera eines benachbarten Sexshops auf der gleichen Frequenz sendeten. Der Besitzer des Etablissements montierte daraufhin seine Kamera ab. Die Kripo war sich nicht sicher, ob der Vorgang „strafrechtlich relevant" sei. Weshalb auf der Überwachungskamera Pornofilme liefen, ging aus der Mitteilung nicht hervor (Im falschen Film, SZ 13.12.2013, 34).

Hamburg

„Gefahrengebiet" mit Personenkontrollen nach Randale

Am 13.01.2014 hob die Polizei Hamburg ein von ihr am 04.01.2014 eingerichtetes Gefahrgebiet wieder auf. Begründet wurde die Einrichtung damit, dass bei Krawallen in den vorangegangenen Wochen wiederholt Angriffe auf Polizeibeamte und öffentliche Einrichtungen wie zum Beispiel Polizeigebäude stattgefunden hätten. Zuvor hatten am 29.12.2013 nach Polizeiangaben etwa 50 mutmaßlich linksextremistische Angreifer die Davidwache auf der Reeperbahn angegriffen und drei Beamten zum Teil schwer verletzt. Die Staatsanwaltschaft hatte daraufhin eine Ermittlung wegen versuchten Totschlags eingeleitet und für Hinweise auf den Täter wurden 10.000 Euro Belohnung ausgesetzt.

Bei Ausrufung eines Gefahrengebietes darf gemäß dem „Gesetz über die Datenverarbeitung der Polizei" diese ohne richterliche Entscheidung jeden Bürger verdachtsunabhängig überprüfen: „Die Polizei darf im öffentlichen Raum in einem bestimmten Gebiet Personen kurzfristig anhalten, befragen, ihre Identität feststellen und mitgeführte Sachen in Augenschein nehmen, soweit aufgrund von konkreten Lageerkenntnissen anzunehmen ist, dass in diesem Gebiet Straftaten von erheblicher Bedeutung begangen werden und die Maßnahme zur Verhütung von Straftaten erforderlich ist." Das Gesetz war im Jahr 2005 unter CDU-Bürgermeister Ole von Beust verschärft worden, ursprünglich mit dem Ziel, die offene Drogenszene zu verdrängen. Seitdem hatte die Hamburger Polizei mehr als 40 Gefahrengebiete eingerichtet, die meisten aber nur für wenige Stunden, etwa anlässlich von Demonstrationen oder Fußballspielen - zuletzt am 21.12.2013, dem Tag, an dem es bei einer Großkundgebung für den Erhalt der „Roten Flora" zu erheblichen Ausschreibungen gekommen ist.

Die Einrichtung des Gefahrengebietes verfolgte das Ziel, so die Polizei, „durch die erweiterten Kontrollbefugnisse für die Polizei, Straftaten von erheblicher Bedeutung in dem Gebiet zu verhindern, um die Bürgerinnen und Bürger und in diesem Fall auch die Polizeibeamten besser zu schützen". Erfasst war ein Teil der Innenstadt, in der 82.000 Menschen leben. Die positive Entwicklung im Gefahrengebiet habe dann dazu geführt, das Gebiet am 09.01.2014 auf die Umgebungen der Polizeikommissariate 15, 16 und 21 zu reduzieren. Bis dahin waren nach Polizeiangaben mehr als 800 Menschen überprüft und „pyrotechnische Gegenstände und Vermummungsmaterial" sichergestellt worden. Gegen 90 Kontrollierte wurden Aufenthaltsverbote ausgesprochen. Außerdem gab es eine Festnahme und mehr als 40 Ingewahrsamnahmen, nachdem sich am 06.01. etwa 300 Menschen über das Internet zu einem „Spaziergang durch das Gefahrengebiet" verabredet hatten.

In den kleineren Gefahreninseln wurde nur noch nachts zwischen 18:00 und 06:00 kontrolliert. Die Kontrollen hatten nach Ansicht der Polizei eine positive Entwicklung zur Folge. Es habe u.a. keine weiteren gezielten Übergriffe auf Polizeibeamte gegeben. Damit sind die mit der Einrichtung der Gefahrengebiete verfolgten Ziele erfolgreich erfüllt worden. Im Rahmen der täglichen intensiven Lagebewertung der Polizei wurde ein Fortbestand der Gefahrengebiete nicht mehr für erforderlich angesehen und diese wurden aufgehoben.

Viele Hamburger BürgerInnen hatten auf die Einrichtung der Gefahrengebiete mit „Spaziergängen" und Demonstrationen in den betroffenen Straßen protestiert. Zuletzt hatten sich am Dienstagabend knapp 600 Menschen aus dem linken Spektrum im Stadtteil St. Pauli getroffen, um gegen die Sonderrechtszonen zu demonstrieren. Zwar kam es

zu vereinzelten Böllerwürfen, ansonsten blieb die spontan angemeldete Kundgebung aber friedlich. Die Einrichtung der Sperrzone führte in der Politik vor allem von Seiten der Grünen, der FDP und der Linken zu kritischen Reaktionen. Die Grünen kritisierten, das Gefahrengebiet führe zu einem „Generalverdacht“ und zu einer „massiven Einschränkung der Bewegungsfreiheit für viele Tausende Menschen. Beschränkt würde die Versammlungsfreiheit und das Recht auf informationelle Selbstbestimmung. Wegen der erheblichen Größe des Gebietes müsse die Verhältnismäßigkeit überprüft werden. Der innenpolitische Sprecher der FDP-Fraktion Carl-Edgar Jarchow ergänzte, das Gebiet dürfe nur so lange ausgewiesen werden, wie es die Lage erfordere. Am 06.01. befasste sich der Innenausschuss der Hamburgischen Bürgerschaft mit der umstrittenen Maßnahme.

Die in der Hansestadt alleinregierende SPD und die Polizei betonten, dass der rechtliche Rahmen ausgeschöpft wurde. Auch die oppositionelle CDU sprach sich für die verdachtsunabhängigen Kontrollen aus. Innensenator Michael Neumann (SPD) verteidigte die Einrichtung des Sperr- und Kontrollgebiets: „Die Einrichtung des Gefahrengebiets als Reaktion auf die massive Gewalt gegen Polizisten und Gebäude war richtig und notwendig.“ Die Polizei werde auch künftig „konsequent und mit Augenmaß auf die weitere Entwicklung reagieren“. Hamburgs Bürgermeister Olaf Scholz (SPD) assistierte: Zweifel an der Verfassungsmäßigkeit des Polizeigesetzes habe er nicht. Damit werde „sehr flexibel, souverän und wenig aufgeregt umgegangen. Ganz viele Bewohner fühlten sich sicherer.“ Es sei Aufgabe der SPD, für Recht und Ordnung zu stehen: „Leute, die das nicht mögen, finden es eben nicht gut.“ Mit dem öffentlichen Druck habe die Reduzierung und dann die Auflösung des Sondergebietes nichts zu tun gehabt.

Im Nachhinein erwies sich, dass Polizeipräsident Wolfgang Kopitzsch wissentlich von Anfang an unberechtigterweise linksextremistische Autonome für den Angriff auf die Davidwache in St. Pauli vom 28.12.2013 verantwortlich machte, indem er meinte: „Gewalt als Mittel zur Durchsetzung politischer Ziele ist völlig ungeeignet und kontraproduktiv.“ In einem internen Papier des Landeskriminalamtes vom Januar 2014 finden sich keine Hinweise auf Linksautonome, sondern folgende Passage: „Als sie (die Angreifer, DANA), sich in Höhe der Davidwache befanden, nahmen Polizeibeamte Sprechchöre (u. a. USP-USP) wahr, wie sie sie aus Fußballeinsätzen kennen, weiterhin wurde Pyrotechnik entzündet.“ USP steht für Ultra Sankt Pauli - gewaltbereite Fans des Fußball-Zweitligisten FC St. Pauli. Ein Polizeisprecher erklärte jedoch, er sehe „keinen Widerspruch, da es sich um eine generelle Aussage des Polizeipräsidenten zur Thematik Gewalt“ handelte, „und nicht um ein Ermittlungsergebnis“ (Der Spiegel 4/2014, 15; POL-HH: 140113-1, Scholz rechtfertigt Polizeikontrollen, SZ 13.01.2014, 1, 6; www.hamburg.de 13.01.2014; Polizei verkleinert Gefahrengebiet, www.sueddeutsche.de 09.01.2014; Parnack, Unter Kontrolle, SZ 07.01.2014, 6).

Niedersachsen

Elektronische Fußfessel überführt Täter

Die Polizei hat einen 32-jährigen Fußfessel-Träger nach einem versuchten Mord festgenommen. Der Mann soll zusammen mit einem Komplizen Anfang Januar 2014 eine Seniorin in Hannoversch Münden überfallen haben. Gemäß Polizeiangaben wurde bei der Auswertung der Überwachungsdaten der Fessel festgestellt, dass sich der Drogenabhängige zur Tatzeit am Haus der Frau aufgehalten hat. Das 72 Jahre alte Opfer war von dem Komplizen des Mannes bis zur Besinnungslosigkeit gewürgt worden, ist aber nicht mehr in Lebensgefahr. Der Göttinger Polizeipräsident Robert Kruse sagte: „Die Fußfessel ist kein Allheilmittel, aber sie war sehr hilfreich beim Aufklären dieser schlimmen und schweren Straftat.“

Auf die Spur gekommen sind die Beamten durch Routine-Ermittlungen, bei denen festgestellt wurde, dass der 32-Jährige das Haus der Frau gekannt habe, weil er dort bei einem Umzug geholfen hatte. Mit seiner Fußfessel durfte sich der Mann im Raum Göttingen bewegen und den Tatort erreichen, ohne gegen Auflagen zu verstoßen. Inzwischen sitzt er wegen Raubes in Untersuchungshaft, sein Mittäter wegen versuchten Mordes. Die Ermittler berichteten, der Drogenabhängige sei seit seinem 16. Lebensjahr kriminell gewesen. Unter anderem sei er wegen zweifachen sexuellen Missbrauchs von Kindern verurteilt worden. Die Fußfessel trug er seit Herbst 2012 auf Anordnung des Amtsgerichtes im thüringischen Arnstadt, um ihm erneute Straftaten zu erschweren (Polizei verhaftet Fußfessel-Träger, http://www.stuttgarter-nachrichten.de 10.01.2014; Mordversuch: Täter mit Fußfessel geht Polizei ins Netz, Kieler Nachrichten 11.01.2014, 12).

Schleswig-Holstein

Privatfahndung im Internet

Die Sylter Rundschau berichtete von einem in mancher Hinsicht klassischen Fall privater Internetfahndung: Ein Sylter, also ein Bewohner der nördlichsten Insel in Deutschland, verlor am 28.12.2013 an einer Tankstelle sein Portemonnaie - seinen Geldbeutel. Die Überwachungskameras der Tankstelle erfassten einen Mann, der den verlorenen Geldbeutel findet, sich bückt und offenbar einsteckt. Der Sylter ließ sich von der Tankstelle die Bilder der Überwachungskameras geben und stellte den vermeintlichen Portemonnaie-Dieb ins Internet - drei Bilder, die den Findevorgang dokumentieren, und drei Kassenbilder mit Gesichtsaufnahmen - auf die Facebookseite der Gruppe Gesucht-Gefunden-Sylt. 5886 Mitglieder dieser Netzgemeinde wurden damit aufgerufen, sich mit dem Eigentümer des Geldbeutels in Verbindung zu setzten, sollten sie den gut erkennbaren Herren auf den Fotos kennen. Auch der Abgebildete wurde höflich angeschrieben: „Lieber Finder, ich darf davon ausgehen, dass Du noch vorhast, meine Geldbörse (...) abzugeben, inklusive Inhalt versteht sich.“ Sollte dies nicht geschehen, werde er in sechs Tagen wegen Fundunterschlagung angezeigt.

Schnell entbrannte in der Netzgemeinde eine heftige Diskussion: „Datenrechtlich verwerflich“ oder „nicht in Ordnung“ fanden einige Nutzende diese Form der öffentlichen Fahndung. Andere sahen es als gerechtfertigtes Mittel, habe der Mann das Portemonnaie doch offenbar unrechtmäßig behalten. Der Eigentümer selbst schrieb: „Über mögliche Konsequenzen bin ich mir vollkommen im Klaren und ich trage auch die alleinige Verantwortung dafür.“

Markus Langenkämper, Pressesprecher der Polizeidirektion Flensburg, signalisierte, dass für die Polizei Facebook als Ermittlungsmöglichkeit ein zweischneidiges Schwert sei. Den Sylter Weg halte er aber erst recht für „sehr problematisch“. Aus mehreren Gründen: Die Tankstelle dürfe zwar Bilder aus ihren Überwachungskameras herausgeben, „aber nur zur Strafverfolgung“. Dass der Eigentümer die Fotos auf Facebook veröffentlicht hat, sieht Langenkämper als „Form der Nötigung“ – nicht zuletzt deshalb, weil gerade nach zwei Tagen auch noch die Chance bestand, dass der Finder plant das Portemonnaie abzugeben. Sollte dieser sich an der Veröffentlichung auf Facebook stören, könnte er mit einer Unterlassungsklage einreichen.

In anderen Fällen greift die Polizei selbst zum sozialen Netzwerk, um nach Hinweisen für die Polizeiarbeit zu suchen. Im Falle des im Herbst 2013 verschwundenen 17-jährigen Marco in Lübeck beispielsweise wurde nach dem Jungen auch auf Facebook gesucht. In diesem Fall hatten die Eltern ihr Einverständnis gegeben, dass das Bild ihres Sohnes dort veröffentlicht wird. Und im neuen Jahr fahndet die Grömitzer Polizei im sozialen Netzwerk nach zwei Männern, die in der Silvesternacht einen anderen brutal zusammengeschlagen haben – allerdings via Täterbeschreibung, ohne Bilder. In kürzester Zeit wurde dieser Aufruf über 1000 Mal geteilt. Für die Polizei ist Facebook eine Möglichkeit, möglichst viele Menschen schnell zu erreichen. Trotzdem: Von „Selbstjustiz“ wie im Sylter Fall rät Langenkämper ausdrücklich ab. Fahnden solle dann doch nur die Polizei.

Björn Nielsen, einer der Administratoren von Gesucht-Gefunden-Sylt verwahrte sich dagegen, dass auf seiner Seite gefahndet oder vorverurteilt wurde: „Da wurde einfach nur der Finder gesucht.“ Das nächste Mal werde er aber den Eintrag wohl schneller löschen lassen. Das Portemonnaie blieb übrigens vorläufig - laut Facebook - verschwunden. Der Eigentümer wollte sich gegenüber der Lokalpresse nicht äußern: Das sei ihm dann doch zu viel Öffentlichkeit.

Aus datenschutzrechtlicher Sicht dürfte schon die Film-Weitergabe von der Tankstelle an den Verlierer unzulässig gewesen sein. Dieser kann zwar ein rechtliches Interesse für sich geltend machen, doch standen wegen der beabsichtigten Internetveröffentlichung überwiegende Drittinteressen entgegen. Die Veröffentlichung durch den Sylter war demgemäß auch nicht in Ordnung. Interessant ist, dass der Fahndungsaufruf im Netz viele kritische Stimmen erntete, die letztlich zu dessen Löschung führten. Die soziale Kontrolle im Netz hat hier funktioniert. Der Weg über die Polizei hätte eine klassische Ermittlung ermöglicht - die Feststellung des tankenden Finders über sein Kfz-Kennzeichen, das bei der Videokontrolle erfasst wird (Reußner, Sylter startet Privatfahndung im Netz, www.shz.de 04.01.2014).

Datenschutznachrichten aus dem Ausland

UNO

UN-Generalversammlung beschließt vage Resolution zum Datenschutz

Die UN-Generalversammlung hat im Dezember 2013 eine von Deutschland und Brasilien initiierte Resolution für effektiven Datenschutz im digitalen Zeitalter angenommen. Die Formulierungen wurden zuvor auf Drängen der USA mehrfach aufgeweicht.

Die Resolution „The right to privacy in the digital age“ („Das Recht auf Datenschutz im Digitalen Zeitalter“) ergänzt den UN-Zivilpakt. Dieser regelt die bürgerlichen und politischen Rechte von Bürgern der UN-Vertragsstaaten. Die Resolution ist völkerrechtlich nicht bindend und könnte ausschließlich symbolische Wirkung entfalten. Die Vertragsstaaten werden in der Resolution dazu aufgerufen, die Datenschutzrechte der Bürger zu respektieren und Datenschutzverletzungen zu beenden. Unabhängige Kontrollmechanismen sollen eingeführt und Transparenz und Verantwortlichkeit hergestellt werden. Es wird auch ein UN-Bericht über die Folgen der Überwachung gefordert, der 2014 dem Menschenrechtsausschuss und der Vollversammlung vorgelegt werden soll.

Die Einflussnahme der USA ist aus einem öffentlich gewordenen, ursprünglich als geheim eingestuften Papier mit der Überschrift „U.S. Redlines“ deutlich zu erkennen. Es geht also um Toleranzschwellen der USA. In dem Dokument heißt es:

Die Resolution dürfe nicht Überwachung im Allgemeinen, sondern nur „ungesetzlicher Überwachung gelten“. Die „bekannt gewordenen Tätigkeiten“ der US-Regierung seien legal gewesen.

Eine „rechtmäßige“ Überwachung bedeute nicht automatisch eine Verletzung der Meinungsfreiheit.

Es werde der Anschein erweckt, dass Staaten auch Datenschutzrechte von Ausländern wahren müssten. Dies entspreche nicht dem Verständnis der USA von den Regelungen des UN-Zivilpakts.

Mit ihren Forderungen haben sich die USA teilweise durchgesetzt. So wird die Überwachung des Internetverkehrs zum Beispiel nicht mehr in jedem Fall als Menschenrechtsverletzung betrachtet. Gegen die Aufweichung des Textes hatten zuvor die Menschenrechtsorganisationen Amnesty International, Electronic Frontier Foundation, Privacy International, Human Rights Watch und Access in einem offenen Brief protestiert, offenbar erfolglos.

(Martin Holland, NSA-Affäre: UN-Generalversammlung beschließt Resolution für mehr Datenschutz, www.heise.de 19.12.2013; Martin Holland, NSA-Affäre: UN-Resolution für mehr Datenschutz einstimmig angenommen www.heise.de 27.11.2013; Michael König, Vage ist nicht vage genug, www.sueddeutsche.de 22.11.2013)

Weltweit

Akademiker-Aufruf gegen Massenüberwachung

Etwa 250 DozentInnen aus der Europäischen Union (EU), den USA und Australien unterzeichneten den Aufruf „Academics Against Mass Surveillance“, der am 02.01.2014 online gegangen ist (www.academicsagainst surveillance.net/). Unter den Unterzeichnenden sind Ulrich Beck von der Universität München, Neil Richards von der Washington University in Saint Louis und Andrew Roberts von der Melbourne Law School. Der Appell fordert das Recht auf Privatsphäre als Grundrecht, welches in internationalen Verträgen wie der Europäischen Konvention der Menschenrechte und der internationalen Vereinbarung der bürger- und politischen Rechte festgeschrieben ist. Ohne Privatsphäre könnten, so die Unterzeichnenden, die freie Meinungsäußerung und der freie Informationsaustausch nicht garantiert werden. Der Appell versteht sich nicht als Konkurrenz zu den Aufrufen, die zuvor SchriftstellerInnen und RechtsanwältInnen veröffentlicht hatten (DANA 4/2013, 155 ff.). Er ist mit diesem in den zentralen Punkten identisch und soll das Bewusstsein schärfen, dass jede individuelle Privatheit gefährdet ist.

Initiiert wurde der Aufruf unter anderem von Beate Roessler von der Universität Amsterdam – angesichts der Tatsache, dass weder im niederländischen Parlament noch in der Öffentlichkeit allgemein bisher eine Debatte über die NSA-Affäre stattgefunden hatte. Die internationale Öffentlichkeit soll daran erinnert werden, dass sich die Aktivitäten der NSA gegen die Privatheit jedes Einzelnen richten – jeder einzelne Bürger werde dabei, erklärt Roessler, als potentieller Terrorist gewertet: „Wir wollen, dass dieses Thema in allen Öffentlichkeiten wie Netzwerken und Zeitungen besprochen wird.“ Die Unterzeichnenden der Erklärung rufen die nationalen Parlamente auf, aktiv in die Debatte einzusteigen und Gesetzesänderungen anzugehen. Staatliche Geheimdienste müssten zu Transparenz und Verantwortlichkeit verpflichtet werden, das Abhören von Telefon, E-Mail, Facebook und finanziellen Transaktionen müsse ein Ende haben. Die Öffentlichkeit dürfe nicht einer allumfassenden Massenüberwachung der staatlichen Geheimdienste unterliegen (Bachmann, Neuer Aufruf gegen die NSA, www.sueddeutsche.de 04.01.2014; SZ 04.-06-01.2014, 12).

Europa

SIS I gehackt

Im Jahr 2012 drangen Hacker in die Computer eines Dienstleisters ein, der den dänischen Teil des Schengener Informationssystems betrieb. Das Schengener Informationssystem (SIS) - eine gemeinsame Datenbank europäischer Polizeibehörden - beinhaltet Daten über Fahndungslisten, Einreiseverbote und überwachte Fahrzeuge. Jede nationale Datenbank enthält dabei alle Daten aus dem gesamten Schengenraum. Die Hacker fanden Polizeiinformationen aus 28 Ländern sowie von Europol und Eurojust. 1,2 Millionen Datensätze wurden aus dem SIS kopiert. Der Vorfall blieb lange Zeit nichtöffentlich. Erst im März 2013 informierte die EU-Kommission die Schweizer Polizei. Andere Schengen-Mitgliedstaaten wurden sogar erst im Juni 2013 von der dänischen Polizei informiert. Ende Dezember 2013 berichteten Schweizer Medien über den Vorfall.

Die Bundesregierung räumte nun ein, dass auch 272.606 Datensätze deutscher Polizeibehörden kopiert wurden. Die Zahl nannte der Parlamentarische Staatssekretär Ole Schröder am 16.01.2014 auf eine Frage des Linken-Abgeordneten Andrej Hunko. Schröder teilte mit, dass es sich bei den Angreifern um einen schwedischen und einen dänischen Hacker gehandelt habe. Auf einem ihrer Rechner sei „eine Vielzahl anderer heruntergeladener Daten“ gefunden worden, was dafür spreche, dass die Täter es nicht gezielt auf SIS-Daten abgesehen hätten. Ob diese Daten weitergegeben oder veröffentlicht wurden, sei der Bundesregierung nicht bekannt. Die Sicherheitslücke, die 2012 das Einfallstor für die mutmaßlichen Täter gewesen war, sei inzwischen geschlossen worden. Details zum Angriff habe die dänische Polizei aber nicht bekannt gegeben.

In der Schweizer Presse war zu lesen, dass die Daten codiert gewesen seien, sodass man wissen muss, welcher Zahlencode zu welcher polizeilichen Maßnahme gehört, um mit den Daten wirklich etwas anfangen zu können. Kryptografisch verschlüsselt aber waren die Daten nicht. Betroffen von dem Angriff war das SIS der ersten Generation. Seit April 2013 ist SIS II in Betrieb, es enthält unter anderem biometrischen Daten wie Fotos, Fingerabdrücke und DNA-Proben. Erst kurz danach hat auch die Bundesregierung von dem Angriff auf die alte Version des SIS erfahren. Sie habe den Vorfall aber nicht öffentlich gemacht, so Andrej Hunko, um SIS II „nicht zu diskreditieren“ (Beuth, Hacker kopieren 270.000 Datensätze der deutschen Polizei, www.zeit.de 17.01.2013)

Europa

Bericht zur Durchsetzbarkeit des Datenschutzes in Europa veröffentlicht

Die EU-Grundrechteagentur hat am 27. Januar 2014 einen Bericht zum Datenschutz veröffentlicht, der ein

mangelndes Bewusstsein der Opfer für Datenschutzverstöße und vorhandene Rechtsmittel offenbart. Die EU-Grundrechteagentur (European Union Agency for Fundamental Rights – FRA), ein unabhängiges Beratungsgremium der EU, hat für diesen Bericht Erfahrungen mit der Zugänglichkeit und Effektivität von Beschwerdemöglichkeiten und gerichtlichem Rechtsschutz gemessen. Hierzu wurden in einer groß angelegten Untersuchung Betroffene von Datenschutzverletzungen, Mitarbeitende aus Aufsichtsbehörden, Anwälte, Richter und Vertreter der Zivilgesellschaft zu ihren Einsichten befragt. In 16 EU-Staaten wurden mehr als 700 Personen, davon 46 in Deutschland, interviewt.

Die Mehrzahl der Opfer von Datenschutzverletzungen wendet sich dem Bericht nach an Datenschutzbehörden. Häufig wollen sie damit verhindern, dass ähnliche Verletzungen erneut geschehen; eine finanzielle Entschädigung steht dabei nicht im Vordergrund. Nur in Ausnahmefällen beschreiten Opfer den Rechtsweg. Gerichtsverfahren gelten als zu kompliziert, kostspielig und zeitaufwendig. Fehlende Rechtshilfe, ein Mangel an Datenschutzspezialisten sowie mit zu geringen Ressourcen ausgestattete Datenschutzbehörden und Mittlerorganisationen werden als Problem gesehen. Aus Sicht der Befragten existieren zu wenige Informationen über Datenschutzverfahren und Rechtsbehelfe.

„Es ist heute schlichtweg zu einfach, die personenbezogenen Daten von europäischen Bürgerinnen und Bürgern zu erfassen und zu missbrauchen. Diese Verstöße können tiefgreifende Folgen für die Opfer von Datenschutzverletzungen nach sich ziehen“, erklärte FRA-Direktor Morten Kjaerum: „Es ist an der Zeit, die Datenschutzbehörden zu berechtigen, diesen Verletzungen entgegenzuwirken, damit die Opfer angemessene Entschädigungen erhalten können.“

Gestützt auf ihre Forschungsergebnisse schlägt die FRA folgende Maßnahmen zur Verbesserung des Status-quo vor:

- Sensibilisierung der Öffentlichkeit für Beschwerdemechanismen, einschließlich der nationalen Datenschutzbehörden und ihrer Aufgaben;
- Schulungen zum Thema Datenschutz für Juristen, so dass diese fundierte Beratung bieten können;
- Stärkung der Unabhängigkeit der Datenschutzbehörden;
- Bereitstellung angemessener Ressourcen und Befugnisse für Datenschutzbehörden, um Datenschutzverletzungen entgegenzuwirken;
- finanzielle Förderung von Organisationen der Zivilgesellschaft und unabhängigen Einrichtungen, die die Opfer bei der Wahrnehmung ihres Rechts auf Wiedergutmachung unterstützen;
- Vereinfachung der Regeln zur Beweislast, insbesondere für Fälle im Online-Bereich, um es Privatpersonen einfacher zu machen, ihren Fall vor Gericht zu bringen oder eine Aufsichtsbehörde anzurufen.

Die vorgeschlagene Reform der EU-Datenschutzvorschriften trägt aus Sicht der FRA dazu bei, diese Probleme zu verringern. Die Vizepräsidentin der Europäischen Union und Kommissarin für Justiz, Viviane Reding, sagte hierzu: „In der Europäischen Union ist Datenschutz ein Grundrecht. Wir müssen sicherstellen, dass dieses Recht geschützt ist und dass die Bürger es durchsetzen können. Wie der Bericht der EU-Agentur für Grundrechte zeigt, wissen nach wie vor viele Bürger nicht, an wen sie sich wenden müssen, wenn ihre Daten missbraucht wurden. Dies ist inakzeptabel.“ Reding forderte die EU-Ministerinnen und -Minister auf, die Datenschutzreform rasch umzusetzen.

In Deutschland wurde die Forschung vom Deutschen Institut für Menschenrechte e. V. durchgeführt – einem nationalen, aus dem Bundeshaushalt verschiedener Ministerien finanzierten Institut zur Förderung und zum Schutz der Menschenrechte. Zu den Ergebnissen in Deutschland äußerte sich das Institut in seiner Presseerklärung vom 27.01.2014. Zwar nutzten Betroffene häufig ihre Beschwerdemöglichkeiten bei Datenschutzbehörden, überschätzen aber teilweise deren Möglichkeiten. Angesichts knapper Ressourcen und begrenzter Kompetenzen lassen sich insbesondere komplexe Fälle oder Konflikte mit öffentlichen Stellen nicht immer abschließend durch die Datenschützer klären. Das Menschenrechtsinstitut schloss sich der Forderung der EU-Grundrechteagentur an, dass die laufenden Verhandlungen zur EU-Datenschutzreform zügig zum Abschluss gebracht werden müssen. Insbesondere die von der Kommission vorgeschlagenen Vorschriften für eine angemessene Ausstattung der Aufsichtsbehörden sowie zu Klagerechten für Datenschutzorganisationen würden aus Sicht des Instituts den Rechtsschutz auch hierzulande erheblich verbessern. (PE European Union Agency for Fundamental Rights, Bürger fordern einen wirksamen und zugänglichen Schutz vor Datenschutzverletzungen, http://fra.europa.eu/de 27.01.2014; PE Deutsches Institut für Menschenrechte, Menschenrechtsinstitut fordert besseren Zugang zum Recht für Betroffene von Datenmissbrauch, 27.01.2014; Deutsches Institut für Menschenrechte, „Zugang zu Datenschutz-Rechtsbehelfen in EU-Mitgliedstaaten“ – eine Studie der EU-Grundrechteagentur, 27.01.2014).

Österreich

Andrea Jelinek ist oberste Datenschützerin

Am 03.12.2013 wurde in Österreich vom Ministerrat die Leitung der neuen Datenschutzbehörde, vormals Datenschutzkommission, festgelegt. Am 10.12.2013 erfolgte die Bestellung durch Entschließung des Bundespräsidenten. Dr. Andrea Jelinek, einst Chefin der Wiener Fremdenpolizei, wird Österreichs oberste Datenschützerin. Zuletzt war sie Stadthauptmann des 3. Wiener Gemeindebezirks. Stellvertreter ist Dr. Matthias Schmidl. Dieser war bisher als wissenschaftlicher Mitarbeiter am Verwaltungsgerichtshof, als Referent im Bundeskanzleramt-Verfassungsdienst sowie als Referent in der Datenschutzkommission tätig. Insgesamt gab es acht Bewerbende für die Leitung, sieben für die Stellvertretung.

Die neue unabhängige Datenschutzbehörde, die ihre Tätigkeit am 01.01.2014 offiziell aufnahm, wird nicht nur als Kontrollstelle zur Überprüfung der Einhaltung von Datenschutzvorschriften fungieren, sondern unter anderem auch für die Führung

von Registrierungsverfahren, die Genehmigung von Datenübermittlungen ins Ausland, die Genehmigung von Datenverwendungen für wissenschaftliche oder statistische Zwecke und die Auskunftserteilung an Bürger zuständig sein.

Sie ersetzt die bisherige Datenschutzkommission im Bundeskanzleramt, die im Zuge der Reform der Verwaltungsgerichtsbarkeit aufgelöst wird. Der Europäische Gerichtshof (EuGH) hatte zuvor mit Urteil vom 16.10.2012 festgestellt, dass die bisherige Organisationsform des Datenschutzes in Österreich nicht die europarechtlich geforderte Unabhängigkeit gewährleistet. Die Leitung wird für jeweils fünf Jahre bestellt (Bestellung der Leitung der Datenschutzbehörde mit Wirksamkeit vom 1. Januar 2014, http://www.dsb.gv.at, 20.12.2013, Datenschutz bekommt eine Chefin, www.wienerzeitung.at 03.12.2013).

Frankreich

Höchststrafe gegen Google wegen vielfältiger Datenschutzverstöße

Die französische Datenschutzbehörde „Commission Nationale Informatique et Liberté“ (CNIL) hat den amerikanischen Internet-Konzern Google wegen Verstößen gegen den Schutz der Privatsphäre ein Bußgeld in Höhe von 150.000 Euro verhängt. Innerhalb von acht Tagen muss Google die 30seitige Entscheidung, die auch die CNIL veröffentlichte, auf der eigenen Homepage veröffentlichen. In der Entscheidung wird festgestellt, dass sich das amerikanische Unternehmen an französisches Recht halten müsse. Dies hatte Google immer in Frage gestellt. Auf mehrere Aufforderungen, sich daran zu halten, hatte Google nicht reagiert. Mit dem Zwang zur Veröffentlichung will die CNIL erreichen, dass die Nutzenden informiert werden. In der Begründung wird ausgeführt, dass die Bürger von dem Unternehmen völlig überfordert und gezielt entmündigt werden. Auf „nicht loyale“ Weise sammle Google die Daten von Nutzenden, die keine Ahnung davon hätten, dass ihre Anfragen gespeichert und wie sie benutzt werden.

Im März 2012 hatte Google die Datensammlung ihrer verschiedenen Dienste zusammengeführt: Suchanfragen, YouTube, Gmail, Google+, Picasa, Drive, Docs, Maps ... Dem mussten und müssen die Nutzenden zustimmen. Das Zusammenlegen der Daten, die von den verschiedenen Diensten kommen, erfolge „ohne legale Basis“. Die Nutzenden werden nicht genügend über „den Zweck und das Ausmaß“ der Datenarchivierung informiert, deshalb seien sie auch nicht in der Lage, ihre Rechte wahrzunehmen. Sie wissen nicht, wie sie sich gegen die Speicherung ihrer persönlichen Vorlieben wehren und ein Löschen der Daten verlangen können. Auch speichere Google Daten für unbestimmte Zeit und lösche sie nicht, wenn sie nicht mehr zu dem ursprünglichen Zweck benötigt würden. Zudem werde es den BürgerInnen erschwert und zuweilen unmöglich gemacht, gespeicherte Daten korrigieren oder löschen zu lassen. Beanstandet wurde weiterhin, dass Google Cookies verwendet, ohne sich an die Bestimmung zu halten. Auch über die Dauer der Archivierung wird nichts gesagt.

Mit den 150.000 Euro, die für Google bei einem Jahresumsatz von 50 Milliarden ökonomisch wenig relevant sein dürften, handelt es sich um die bisher gesetzlich vorgesehene Höchststrafe. Ähnliche Prozesse werden in vielen europäischen Ländern geführt. Im Februar 2013 hatten europäische Datenschutzbehörden beschlossen, Sanktionen zu ergreifen. In Deutschland, Spanien, Großbritannien, Italien und den Niederlanden hat Google wegen der 2012 eingeführten Regeln ebenfalls Ärger. Im Dezember 2013 hat die spanische Datenschutzbehörde AEPD gegen Google eine Geldstrafe von 900.000 Euro verhängt. Hamburgs Datenschutzbeauftrager Johannes Caspar hat im Juli 2013 ein Verwaltungsverfahren gegen den Konzern eingeleitet. Er könnte beispielsweise eine Anordnung erlassen, nach der Google seine Verarbeitungspraxis umstellen muss (Altweg, Höchststrafe für Google, www.faz.net 09.01.20014; Frankreich verhängt Geldstrafe gegen Google, www.heise.de 09.01.2014).

Frankreich

Gesetzlich umfassende Internetüberwachung geplant

In Frankreich wird kontrovers über ein neues Gesetz zur Internetüberwachung diskutiert. Die Nationalversammlung und am 12.12.2013 der Senat haben eine Klausel beschlossen, die Behörden das Abfischen von Verbindungs- und Standortdaten bei Providern und den Zugriff auf Inhaltsdaten bei Diensteanbietern in Echtzeit erlaubt. 164 Senatoren votierten für die einschlägige Initiative der französischen Regierung des sozialistischen Präsidenten Francois Hollande, 146 dagegen. Ein Antrag der Grünen zum Streichen der kritisierten Regelung fand keine Mehrheit.

Gilles Babinet, netzpolitischer Vertreter Frankreichs bei der EU-Kommission, hatte im Vorfeld gewarnt, dass das Land mit dem Vorstoß „an der Schwelle zur digitalen Diktatur“ stehe. Der Unternehmer bezeichnete den Gesetzentwurf als „größten Schlag“ gegen die Demokratie seit vielen Jahrzehnten. Es dürfe auf keinen Fall eine Blanko-Erlaubnis etwa für Sicherheitsbehörden oder das Militär geben, „alles und jeden in Echtzeit abzuhören“. Die „Association des Services Internet Communautaires“ (ASIC), ein gegen die Vorratsdatenspeicherung kämpfender Verband von Internetfirmen wie eBay, Facebook, Google, Microsoft oder Yahoo, forderte die Einschaltung des Verfassungsrats, um die geplante Ausdehnung der Netzüberwachung zu stoppen. Die geplante Zugriffsmöglichkeit auf E-Mails, Fotos oder von Nutzern in der Cloud abgespeicherte Dokumente verstoße gegen EU-Datenschutzbestimmungen und würde das Vertrauen in französische Online-Dienste unterwandern. Ähnlich äußerten sich andere nationale Wirtschaftsvereinigungen.

Es geht um Artikel 13 des Wehrplangesetzes zur Umsetzung der neuen Verteidigungsstrategie der französischen Regierung. Der Gesetzgeber führte die Passage 2006 als zeitlich begrenzte Anti-Terror-Maßnahme ein und verlängerte sie bereits 2008 und 2012. Derzeit gilt sie theoretisch noch bis 2015. Die Klausel erlaubt bislang vor allem Geheimdiensten das Sammeln von

Verbindungsdaten. Mit dem Beschluss wird diese nun entfristet und deutlich ausgeweitet. Berechtigte Behörden, zu denen künftig etwa auch Einrichtungen unter der Leitung des Wirtschafts- und Finanzministeriums wie Steuerämter gehören, dürften demnach zur Strafverfolgung oder zur Abwehr von Gefahren wie Wirtschaftsspionage in Echtzeit auf sämtliche von Zugangsanbietern übertragenen sowie bei Hostprovidern und Webportalen gespeicherten Daten ohne richterliche Genehmigung zugreifen. Über Gesuche soll nur noch ein nationales Kontrollgremium entscheiden.

Präsident Hollande hatte sich wiederholt über die Spionageaktivitäten der NSA und des britischen GCHQ empört, die auch Frankreich im Visier haben. Ihm wird vorgeworfen, die eigenen Sicherheitsbehörden mit vergleichbar weitgehenden rechtsstaatswidrigen Befugnissen auszustatten (Krempl, Scharfe Kritik an Frankreichs neuem Überwachungsgesetz, www.heise.de 12.12.2013).

Niederlande

Datenschützer ermitteln gegen Google

Die niederländische Datenschutzbehörde College Bescherming Persoonsgegevens (CBP) teilte mit, dass dem Internetkonzern Google nun auch in Holland wegen Verletzung der Datenschutzgesetze eine Strafe droht. In ganz Europa steht Google deswegen im Visier der Behörden. Der Konzern verwendet persönliche Daten in einer Reihe von Dienstleistungen, unter anderem bei der Websuche und beim Videoportal Youtube, ohne die Nutzer zu informieren oder im Vorfeld um Erlaubnis zu fragen, so CBP-Chef Jacob Kohnstamm: „Google spinnt ein unsichtbares Netz aus unseren persönlichen Daten, ohne unsere Zustimmung. Und das ist per Gesetz verboten.“ Google wurde zu einer Anhörung eingeladen, auf der beschlossen werden soll, ob weitere Schritte gegen den Suchmaschinenbetreiber eingeleitet werden. Es könnte auch eine Strafe verhängt werden.

Der US-Konzern wird in ganz Europa wegen seiner Handhabung des Datenschutzes unter die Lupe genommen. Behörden mehrerer Länder, darunter Deutschland, Italien und Spanien, untersuchen derzeit die Geschäftspraktiken von Google. Das Landgericht Berlin hat auf Klage der Verbraucherzentrale Bundesverband (vzbv) insgesamt 25 Klauseln der Datenschutz- und Nutzungsbedingungen für rechtswidrig erklärt. In Spanien droht Google eine Strafe von bis zu 1,5 Millionen Euro, in Italien könnten es mehr als 1,2 Millionen werden und in Deutschland drohen 1 Million Euro. Im September 2013 hatte die französischen Datenschutzbehörde CNIL ein Verfahren gegen Google eingeleitet, dass ebenfalls in einer Strafzahlung münden könnte. Google hatte eine dreimonatige Frist zur Anpassung seiner Praktiken zur Behandlung von Nutzerdaten verstreichen lassen (Van Tartwijk, Niederländische Datenschutzbehörde nimmt sich Google vor, www.sueddeutsche.de 29.11.2013; Romberg, Druck auf Google, SZ 21.11.2013, 37).

Großbritannien

Tesco-Supermärkte analysieren Kundengesichter

An 450 Tankstellen der britischen Einzelhandelskette Tesco, so das Branchenblatt The Grocer, sollen bald Kameras KundInnen nicht nur filmen, sondern auch deren Augen digital erfassen. Auf dieser Grundlage entscheidet das Programm Optimeyes, welche kurzen Werbespots ihnen auf einem Bildschirm gezeigt werden. Die britische Datenschutzorganisation Big Brother Watch warnte: „Die Menschen würden nie akzeptieren, dass die Polizei in Echtzeit erfährt, in welche Läden wir gehen, aber diese Technologie kann genau das. Es ist ein Überwachungsstaat an der Ladentür.“ 2012 stellte eine Arbeitsgruppe der EU-Kommission zur Gesichtserkennung fest, dass diese Technik dazu verwendet werden kann, Einzelnen „den Zugang zu Geschäften, Restaurants oder anderen Orten zu verweigern“. Nach Protesten von Datenschützern schaltete Facebook seine Gesichtserkennung 2012 in der EU ab. Die Firma, die Tesco mit dem System Optimeyes beliefert, das aus Gesichtern Konsumwünsche liest, heißt Amscreen. Deren CEO Simon Sugar bestätigte: „Ja, es ist wie aus Minority Report“ - also wie in der Science-Fiction-Kurzgeschichte, bei deren Verfilmung Tom Cruise nach einem Augenscan mit individualisierter Werbung bombardiert wird. Sugar ist gewiss, dass seine Technologie „das Gesicht des britischen Einzelhandels verändern“ wird. Optimeyes bestimme aber nur das Geschlecht und teile Kunden in eine von drei Altersklassen ein. Fotos würden nicht gespeichert. Amscreen gehört Simons Vater, Lord Alan Sugar, der mit der Computerfirma Amstrad reich wurde und sich mit dem Geld in den Fußballklub Tottenham Hotspurs einkaufte.

Biometrieprodukte versprechen nicht nur im Sicherheitssektor, sondern auch im Einzelhandel hohe Steigerungsraten. Hier befinden sich die Gesichtserkennungsprogramme aber noch im Entwicklungsstadium und werden noch nicht zur flächendeckenden Überwachung genutzt. Adidas lässt in einigen Geschäften Geschlecht und Alter per Software erkennen, um Kunden entsprechende Sportschuhe zu präsentieren. In Japan scannen Getränkeautomaten Durstige und bieten ihnen vermeintlich passende Drinks an. Der Einzelhandels- und Tankstellenkonzern Tesco setzt schon seit Langem konsequent auf die Auswertung von Kundendaten, 1995 führte er eines der ersten Kundenkartensysteme in Großbritannien ein. Firmenchef Phil Clarke verkündet auf Konferenzen: „Businessregel Nummer eins: Kenne deinen Kunden.“ Nicht allen KundInnen gefällt dies. Bei Twitter wurde zum Tesco-Boykott aufgerufen. Ein Nutzer kommentierte: „Jetzt ist der richtige Zeitpunkt, in eine Burka zu investieren“ (Brühl, Schau mir in die Augen, Kunde, SZ 05.11.2013, 19).

Großbritannien

Massive Kinderüberwachung an Schulen

Die Organisation Big Brother Watch veröffentlichte Zahlen, wonach 40% aller Schulen in Großbritannien von ihren

SchülerInnen biometrische Daten erheben. Damit gehören die 1,28 Mio. Kinder zu den bestüberwachten der Welt. Hundertausende von ihnen hinterlassen täglich ihren Fingerabdruck in Scannern, die in Schulkantinen und Bibliotheken eingesetzt werden. Ein Drittel der Bildungseinrichtungen fragt die Eltern nicht um Erlaubnis zur Speicherung der biometrischen Daten, obwohl dies gesetzlich gefordert ist. In einigen Regionen überwacht eine Videokamera im Durchschnitt fünf SchülerInnen. Kameras sind teilweise sogar in Umkleideräumen installiert. Viele Eltern scheinen sich eher um die Sicherheit ihrer Kinder als um den Missbrauch der Daten zu sorgen, weshalb es kaum Widerstand gegen die Kontrolle gibt (Der Spiegel 3/2014, 80).

Schweden

Internet-Pranger Lexbase heftig umstritten

In Schweden wurde am 27.01.2014 der Online-Pranger Lexbase eingerichtet, auf dem man über eine Namenssuche oder auf einer Landkarte erfahren konnte, wer in dem Land rechtskräftig verurteilt wurde. Darauf gab es derart massive Kritik, dass der Justiziar der Seite Pontus Ljunggren wegen Todesdrohungen zurücktrat. Auf lexbase.se konnte das Vorstrafenregister jedes schwedischen Bürgers eingesehen werden. Auf einer Karte wurden die Wohnorte aller verurteilten Straftäter als rote Punkte markiert. Eine iOS-App warnte vor Straftätern in der Umgebung. Das Interesse an dieser Suchmaschine war so groß, dass wegen der vielen Zugriffe die Seite teilweise lahmgelegt wurde. Die Betreiber machten sich das Informationsfreiheitsgesetz („Offentlighetsprincipen") zunutze und hatten die Dokumente sämtlicher Gerichtsprozesse in Schweden eingesammelt und elektronisch bereitgestellt. Ljunggren meinte, Transparenz sei eine gute Sache, „wir machen sie nur moderner." Das Angebot stille den Hunger der Schweden nach Informationen und könne Frauen helfen, die vor einem Date herausfinden wollen, ob der Gegenüber wegen Vergewaltigung verurteilt wurde. Besorgte Eltern könnten den Schulweg ihrer Kinder daraufhin überprüfen, ob dort Kinderschänder wohnen. Wie die Informationen auf der Seite genutzt werden, liege nicht in der Verantwortung von Lexbase.

Datenschützer waren anderer Meinung, meldeten die Seite der Polizei. Der Juraprofessor Mårten Schultz zeigte sich überzeugt, dass die Seite gegen Datenschutzgesetze verstößt. Darüber hinaus wurden Adressen gefunden, wo entgegen der Anzeige von Lexbase keine verurteilten Straftäter leben. Die Adressen wurden angezeigt, weil dort die erfassten Personen zur Zeit des Urteils wohnten. Nach einem Umzug blieb der Wohnort markiert. Schultz meinte, hier könne der Straftatbestand der Verleumdung einschlägig werden. Gemäß Presseberichten wurden nicht nur verurteilte Personen erfasst, sondern auch die, deren Verfahren mit einem Freispruch endete. Die Daten wurden umgehend von der Seite abgegriffen und auch an anderer Stelle verfügbar gemacht.

Die schwedische Zeitung Dagens Nyheter enthüllte zeitnah, dass Lexbase-Gründer und Mehrheitseigner Jonas Häger seit 2007 in Schweden keine Steuern bezahlt habe. Vor seinem Rücktritt hatte sein Justiziar dies damit erklärt, dass Häger nur lange „segeln gewesen war". Auf Grund des Drucks der Medien sperrte der Internetbetreiber das „Verbrecher-Google" am 31.01.2014. Die Betreiber suchen nun einen anderen Internetanbieter. Die bürgerliche Justizministerin Beatrice Ask äußerte Besorgnis, dass Personen bloßgestellt würden, die ihre Vergehen verbüßt haben. Ministerpräsident Frederik Reinfeldt meinte, es müsse zunächst eine gesellschaftliche Diskussion in Gang kommen, welche dieser Informationen zugänglich sein müssen (Anwar, Kieler Nachrichten, 01.02.2014, 14; Schweden: Massive Kritik an privatem Internet-Pranger, www.heise.de 29.01.2014).

USA

CIA überwacht internationalen Bargeldverkehr

Die Central Intelligence Agency (CIA), der US-Auslandsgeheimdienst, überwacht internationale Geldtransfers, die über Dienstleister wie Western Union und MoneyGram abgewickelt werden. Das Wall Street Journal und die New York Times berichteten unter Berufung auf mehrere mit dem Programm vertraute RegierungsvertreterInnen und ehemalige Beamte, dass die Informationen, wer wem Bargeld überweist, in großen Datenbanken der CIA landen. Von dieser Massendatenabschöpfung sind auch US-AmerikanerInnen betroffen, obwohl sie vom Auslandsgeheimdienst eigentlich nicht überwacht werden dürfen. Erst im Nachhinein „minimiert" oder „maskiert" die CIA die Informationen über US-BürgerInnen. Das gelte aber nicht, so ein ehemaliger US-Beamter, wenn diese für den Geheimdienst von Interesse sind.

Die richterlichen Genehmigungen für das Überwachungsprogramm erteilt – wie auch beim Prism-Programm der National Security Agency (NSA) – der geheim tagende Foreign Intelligence Surveillance Court (FISC). Die rechtliche Grundlage für die Datensammlung bildet der gleiche Abschnitt des Patriot Act, mit dem auch die NSA ihre massenhafte, verdachtsunabhängige Überwachung von Telefonverbindungen rechtfertigt. Abschnitt 215 erlaubt es den Geheimdiensten, mit einem entsprechenden Gerichtsbeschluss „alle greifbaren Dinge, darunter Bücher, Aufzeichnungen, Papiere, Dokumente und andere Dinge" zu sammeln, sofern sie „relevant" für die Terrorabwehr oder Spionageabwehr sind. Die US-Regierung definiert das Wort „relevant" so weit, dass auch Daten von Millionen von US-BürgerInnen und AusländerInnen erfasst werden dürfen, die nicht wirklich verdächtig sind.

Die Sammlung der Geldtransferdaten soll nach den Anschlägen vom 11.09.2001 begonnen haben. Dienste wie Western Union oder MoneyGram dienen direkten Geld-Überweisungen von einer Person zur anderen. Mit den in Europa üblichen Überweisungen sind sie nicht direkt vergleichbar. Die Dienste werden beispielsweise von MigrantInnen benutzt, um Geld an ihre Familien in der Heimat zu senden. Die Ermittlungen nach den Terroranschlägen vom 11. September 2001 hatten ergeben, dass auch die Attentäter und ihre Komplizen unter anderem Western Union und MoneyGram genutzt hatten, um Geld in die USA zu schicken. Damals arbeitete z. B.

Western Union freiwillig mit der CIA zusammen. Im Jahr 2006 wurde die Zusammenarbeit auf eine gesetzliche Basis gestellt – eben jenen Abschnitt 215 des Patriot Act. Die CIA arbeitet den Berichten zufolge mit dem FBI, der US-Bundeskriminalpolizei, zusammen und leitet z. B. Informationen weiter, wenn diese Hinweise auf mögliche terroristische Aktivitäten innerhalb der USA geben könnten. Außer Western Union und MoneyGram würden auch viele kleinere Unternehmen für Bargeldtransfers zur Zusammenarbeit mit der CIA gezwungen. Sprecher der beiden bekannten Unternehmen bestätigten, Kundendaten auf Basis von US-Gesetzen zu sammeln und herauszugeben. Details dürfe man aufgrund gesetzlicher Bestimmungen nicht nennen. Verschwiegenheitsklauseln sind Bestandteil der Gerichtsbeschlüsse nach Abschnitt 215. Western Union teilte mit, es werde etwa 4% seines Umsatzes im Jahr 2014 investieren müssen, um dem Patriot Act und anderen Vorgaben zur Bekämpfung von Geldwäsche und Terrorfinanzierung nachzukommen.

Die CIA reagierte auf die Enthüllungen mit einer knappen Stellungnahme: „Die CIA schützt das Land und das Recht auf Privatsphäre der Amerikaner, indem sie sicherstellt, dass ihre Aufklärungsaktivitäten sich in Übereinstimmung mit US-Gesetzen auf Auslandsaufklärung und Gegenspionage konzentrieren." Die CIA und das US-Finanzministerium betreiben ein weiteres Programm, in dessen Rahmen Transaktionen zwischen Banken überwacht werden. Hier ist die Society for Worldwide Interbank Financial Telecommunication (SWIFT) betroffen. Auch die NSA interessiert sich für SWIFT-Daten; dem Dienst ist es gelungen, die verschlüsselten Verbindungen zu knacken, auf denen derartige Daten ausgetauscht werden. Das EU-Parlament hatte sich angesichts der NSA-Enthüllungen der vergangenen Monate kürzlich mehrheitlich dafür ausgesprochen, das SWIFT-Abkommen, in dessen Rahmen derartige Daten mit den USA offiziell ausgetauscht werden, zumindest vorläufig auszusetzen (Beuth, CIA überwacht internationale Bargeldtransfers, www.zeit.de 15.11.2013; CIA überwacht internationale Geldtransfers, www.spiegel.de 15.11.2013).

USA

Polizeiliche mobile Gesichtserkennung

Nachdem die US-amerikanische Armee mobile Geräte zur Gesichtserkennung schon seit Jahren nutzt, um gesuchte Personen zu entdecken, wird diese Technik nun auch von der Polizei eingesetzt. Das amerikanische Center for Investigative Reporting berichtet über einen entsprechenden Feldversuch der Polizei in der Region von San Diego im US-Bundesstaat Kalifornien.

Seit Januar 2013 werden dort 133 Galaxy Tablets mit entsprechender Software des Unternehmens FaceFirst eingesetzt. PolizistInnen können damit Gesichter fotografieren, die dann innerhalb von Sekunden mit einer Datenbank verglichen werden, in der bereits verhaftete Kriminelle gelistet sind. Ein Foto und wenige Klicks braucht es, bis die PolizistIn auf ihrem Tablet den Namen der Betreffenden, die Adresse, das Strafregister und Fotos von früheren Verhaftungen sehen kann. Dafür wurden alle Bilder der Verhafteten-Datenbank, in den USA Mugshots genannt, eingelesen. Anhand einiger Parameter wie des Abstandes der Augen zur Nase werden die Fotos verglichen. Das funktioniert gemäß Herstellerangaben auch auf Smartphones.

Das entsprechende Projekt des National Institute of Justice heißt Tactical Identification System. Der Test in San Diego ist nur der Anfang. In den zehn Monaten seit Projektbeginn, so das Center for Investigative Reporting, haben PolizistInnen in Kalifornien 5.629 Abfragen gestartet . Künftig sollen noch ganz andere Bilddatenbanken integriert werden, zum Beispiel die mit den Fotos, die für Führerscheine gemacht wurden. Einer der Polizisten, die das System einsetzen, wird in dem Bericht mit den Worten zitiert: „If you‘re not in a criminal database, you have nothing to hide." Wer in keinem Strafregister stehe, habe nichts zu verbergen und müsse sich davor auch nicht fürchten. Die geplante Ausdehnung auf Fotodatenbanken, die keine Kriminellen enthalten, lässt an dieser Aussage Zweifel aufkommen. Ohne dass Betroffene es bemerken, könnten sie verfolgt und ausgespäht werden. Google beispielsweise hat seine geplante Gesichtserkennungssoftware gestoppt. Auch Facebook wurde in Deutschland wegen einer solchen Funktion abgemahnt.

Der Test in San Diego County wurde ohne eine öffentliche Debatte oder Ankündigung gestartet. Erst nach einer Anfrage der Electronic Frontier Foundation (EFF) gaben die Behörden Informationen dazu heraus. Dabei erklärte die Behörde, unter welchen Umständen überhaupt solche Bilder gemacht werden dürfen. PolizistInnen können die Scanner erstens bei Festnahmen einsetzen, zweitens wenn der oder die Betreffende zugestimmt hat und drittens auch zur Auswertung von Überwachungsmaterial von Videokameras und anderen Quellen. Die EFF nennt die Regeln problematisch und besorgniserregend. Es wird den PolizistInnen überlassen, ob sie die Fotos, die sie gemacht haben, wieder löschen. Tun sie das nicht, bleiben die Bilder in den Tablets gespeichert. Das FBI will im Jahr 2014 seine Datenbank, in der mehr als 100 Millionen Menschen gespeichert sind, auf Gesichtserkennung umstellen. Das Programm heißt Next Generation Identification – die nächste Generation des Identifizierens. Für die BürgerrechtlerInnen der EFF ist das eine „Militarisierung der amerikanischen Strafverfolgung" (Biermann, Polizei in San Diego testet Gesichtserkennung, www.zeit.de 08.11.2013).

USA

Millionenstrafe für Google wegen Safari-Cookies

Google muss auf Grund eines Vergleichs mit den Generalstaatsanwälten zahlreicher US-Bundesstaaten eine Strafe in Höhe von 17 Mio. US-Dollar (13 Millionen Euro) dafür zahlen, dass das Unternehmen mithilfe von Cookies das Surfverhalten von Nutzenden des Apple-Browsers Safari erfasste. Der Internetkonzern wird damit zum zweiten Mal zur Kasse gebeten, weil er die Privatsphäre von Safari-Nutzenden verletzte. New Yorks Generalstaatsanwalt Eric Schneiderman erklärte am 18.11.2013: „Indem Google das Surfverhalten von Millionen

Leuten erfasst hat, hat das Unternehmen nicht nur deren Privatsphäre verletzt, sondern auch deren Vertrauen.“ Google hatte Cookies beim Safari-Browser für iPhone, iPad und PC ohne Zustimmung der Nutzenden abgelegt. Das sind kleine Dateien, mit denen sich das Verhalten im Netz teilweise nachverfolgen lässt, was vor allem für Werbetreibende hochinteressant ist. Google verdient sein Geld mit der Platzierung von grafischen Werbeanzeigen auf Websites sowie mit Textanzeigen passend zu den Ergebnissen seiner Suchmaschine. Nach Ansicht der Staatsanwälte hatte Google von Juni 2011 bis Februar 2012 mit seinem Vorgehen die Safari-Einstellungen ausgehebelt. Wegen des Falls hatte der Konzern Mitte 2012 schon eine Buße von 22,5 Millionen Dollar an die US-Handelsbehörde FTC zahlen müssen (Google muss für illegale Safari-Cookies zahlen, www.welt.de 19.11.2013).

USA

Google kauft Nest Labs

Google kauft mit Nest Labs für 3,2 Milliarden Dollar (2,34 Mrd. Euro) eine Firma, die Thermostate und Rauchmelder herstellt. Nest Labs ist Hersteller solcher besonders schicker, smarter Sensoren und Wirkgeräte. Zudem hat die Firma attraktives Personal: 2010 gründeten Matt Rogers mit seinem früheren Kollegen Tony Fadell in Palo Alto im Silicon Valley die Firma. Beide hatten zuvor bei Apple an der Weiterentwicklung des mobilen Musikplayers iPod gearbeitet. Fadell war mitverantwortlich für das Design des iPod und des ersten iPhone. In Sachen sexy Geräte liegt Google nach wie vor deutlich hinter Apple zurück. Nach Ansicht des US-Techblogger John Gruber geht es Google bei dem Kauf auch um die Fähigkeit, „allgemein Hardware für Endkunden richtig hinzukriegen.“ Google geht hin zur Hardware, ohne sich von der Software zu entfernen. Die Übernahme von Nest schließt sich an mehr als zwölf andere an, die Google allein im Jahr 2013 im Hardware-Sektor getätigt hat. Aus dem Suchmaschinen-Unternehmen wird ein immer breiter aufgestellter Universalkonzern, der die Zukunft von Smartphones (Motorola), Tablets, Computern, Brillen, Autos (Audi), Robotern (Boston Dynamics) und möglicherweise bald auch unsere Haushalte entscheidend prägt.

Doch das ist offensichtlich nur ein Grund. Nest hat noch etwas anderes anzubieten, was Google seit Jahren anstrebt: Daten aus Millionen Haushalten. Nest-Thermostate und -Rauchmelder erfassen eine Vielzahl von Informationen darüber, was in einem Haushalt gerade geschieht. Sie merken sich, wann der Nutzer die Temperatur hochregelt, wann herunter. Dank eingebauter, selbstlernender Sensoren für „Temperatur, Aktivität, Luftfeuchtigkeit und Helligkeit“ (Nest-Website) kann der Thermostat sogar erraten, wann jemand zu Hause ist, in welchem Raum sich gerade jemand aufhält. Steuern lässt er sich auch über eine Smartphone-App. Fadell beschreibt seine Vision: „Jedes Mal, wenn ich einen Fernseher einschalte, liefert das die Information, dass jemand zu Hause ist. Wenn sich die Kühlschranktür öffnet, ist das ein weiterer Sensor, weitere Information.“ Nest soll alles über einen Haushalt wissen, was sich nur irgend herausfinden lässt, und es für die Temperaturregelung nutzen.

Das US-Technikblog „GigaOm“ schrieb so auch folgerichtig: „Wenn Google den Nest-Deal abschließt, werden Datenschutzthemen im Zusammenhang mit dem ‚Internet der Dinge‘ erst richtig abheben.“ Die total vernetzte Zukunft mit IP-Adressen für jedes Gerät ist der Alptraum von Datenschützern, was auch Nest bewusst ist. Auf deren Website ist zu lesen: „Unsere Datenschutzerklärung beschränkt die Nutzung von Kundendaten auf die Verbesserung unserer Produkte und Dienste. Wir nehmen Datenschutz ernst, und das wird sich nicht ändern.“ Mit einer derart schwammigen Formulierung bindet sich das Unternehmen aber nicht wirklich und eröffnet sich jede Auswertung und Verknüpfung. Als ein Reporter bei Fadell nachfragte, ob sich die Datenschutzregelung ändern werde, antwortete der Nest-Gründer: „Ich werde nicht niemals sagen.“

Google sieht zweifellos die Big-Data-Möglichkeiten von Nest. Informationen über die Lebensgewohnheiten von Millionen Menschen, gepaart mit all dem, was der Konzern dank seiner Suchmaschine, dank Cookies, GMail und Android schon jetzt über Abermillionen von Menschen weiß - das ist ein wertvoller Schatz. Ein Android-Nutzer, der sich auch noch Nest-Thermostate ins Haus holt, wird Google mehr Informationen über sich und sein Privatleben geben, als jemals ein Konzern über einzelne Personen besessen hat. Fadells Vision passt perfekt zur Vorstellung Googles von der Zukunft des vernetzten Hauses. Schon im Mai 2011 hatte der Konzern verkündet, das eigene Mobil-Betriebssystem Android solle auch für Haus- und Gartentechnik geöffnet werden. Damals schwärmten Google-Manager von den Möglichkeiten vernetzter, intelligenter Haushaltsgeräte. Und schon vorher hatte der Konzern ein Projekt für Smart Meter, intelligente Stromzähler aufgesetzt. Der PowerMeter wurde jedoch 2011 beerdigt, und aus der Android-Revolution zu Hause ist bislang nicht viel geworden.

Nest ist mit einer ähnlichen Vision, gepaart mit hübscher Hardware, sehr erfolgreich. Nest-Thermostate verkauften sich schon Anfang 2013 in Stückzahlen von 40.000 bis 50.000 pro Monat. Ein Nest-Thermostat kostet 250 Dollar. Attraktiv finden das offenbar auch andere. Auf der Technikmesse CES in Las Vegas Anfang 2014 hat Daimler eine Kooperation mit Nest bekanntgegeben. In Europa kann man die Luxusthermostate bislang nicht kaufen. Dafür aber die Konkurrenzprodukte Tado, eQ3-Max oder AlphaEos, ebenfalls intelligente Thermostate, die sich wie Nest auch über eine Smartphone-App steuern lassen (Stöcker, Nest-Übernahme: Google will in Ihr Schlafzimmer, www.spiegel.de 14.01.2014; Paukner, Google kauft sich ein bisschen Zukunft, www.sueddeutsche.de 14.01.2014; Beuth, Google will Dein Mitbewohner werden, www.zeit.de 14.01.2014; Martin-Jung/Paukner, Ein Netz für alles, SZ 15.01.2014, 17).

USA

Bundesgericht erlaubt verdachtslose Laptop-Grenzkontrolle

Ein US-Bundesgericht hat eine Klage gegen die Untersuchung elektronischer Geräte an den Grenzen der USA abgewiesen. Bundesrichter Edward R. Korman entschied, dass die Regierung Lap-

tops, Kameras und ähnliche Geräte von Reisenden ohne einen konkreten Verdacht durchsuchen dürfe. Die American Civil Liberties Union (ACLU), weitere Organisationen und ein Student, dessen Laptop an der US-Grenze beschlagnahmt worden war, hatten das Department of Homeland Security im Jahr 2010 vor dem New Yorker Gericht verklagt. Sie hatten argumentiert, verdachtslose Durchsuchungen von Geräten, die große Mengen persönlicher Daten enthalten, widersprächen dem Standard des vierten Zusatzartikels zur Verfassung. Berufung ist möglich. Richter Korman begründete seine Entscheidung damit, dass im 21. Jahrhundert die gefährlichste Schmuggelware oft in Laptops und anderen elektronischen Geräten enthalten sei – zum Beispiel terroristisches Material und Kinderpornografie (US-Richter: Laptops dürfen auch ohne Verdacht durchsucht werden, www.heise.de 01.01.2014; http://aclu.org/sites/default/files/assets/abidor_decision.pdf).

USA

23andMe Gentest-Firma zwischen Verbot und Verheißung

Testverkauf „unverzüglich einstellen“

Dem Unternehmen 23andMe, dem eng mit dem Suchmaschinen-Giganten Google verbundenen Start-up mit Sitz in Mountain View/Kalifornien, wurde Ende November 2013 von der US-Lebensmittel- und Pharmabehörde Food and Drug Administration (FDA) der weitere Verkauf von DNA-Selbsttest-Sets untersagt. Da die erforderlichen Zulassungen fehlten, gebe es keine Sicherheit, dass die Test-Ergebnisse korrekt seien. Die Behörde befürchtet deshalb Fehldiagnosen, die einerseits Menschen mit erhöhtem Risiko von Erbkrankheiten falsche Sicherheit geben – und andererseits ungefährdete Kunden zu kostspieligen oder gefährlichen Behandlungen verleiten könnten. Die Testergebnisse könnten die KundInnen zu Kurzschlusshandlungen veranlassen, etwa ein Medikament eigenmächtig abzusetzen, weil es angeblich nicht zum Erbgut passt. Würde ein erhöhtes Krebsrisiko unterstellt, so könnten aufwändige und möglicherweise riskante Untersuchungen veranlasst werden. Schon seit Längerem steht 23andMe gegenüber der FDA in der Pflicht, Aussagekraft, Sicherheit und Relevanz der Tests zu belegen. In einer kurzen Stellungnahme anerkannte 23andMe, die Anforderungen der FDA bisher nicht erfüllt zu haben und versicherte, sich sehr darum zu bemühen, die Bedenken der Behörde auszuräumen.

Das Angebot des Unternehmens

Das Unternehmen schickt sich seit einigen Jahren an, die weltgrößte Datenbank für menschliches Erbgut aufzubauen. Die 2006 gegründete Firma gehört weltweit zu den Marktführern im Sammeln und Auswerten von Gen-Daten. Für 99 Dollar konnte dort bisher jeder per Postversand seine DNA auf Erbkrankheiten analysieren lassen. 450.000 KundInnen - auch aus Deutschland - haben das schon getan. Dazu müssen eine wenige Utensilien im Internet bestellt werden. Es wird in ein Röhrchen gespuckt, das an das Unternehmen gesendet wird. Wenig später kann man seine Ergebnisse mithilfe eines Passwortes online abrufen. Firmenchefin von 23andMe ist Anne Wojcicki, inzwischen getrennt lebende Ehefrau des Google-Mitbegründers Sergej Brin. Brin hatte bei sich selbst mit Hilfe von 23andMe ein erhöhtes Parkinson-Risiko festgestellt.

Die Unternehmenssprecherin Catherine Afarian beschrieb gegenüber dem FAZ-Journalisten Richard Gutjahr die Tätigkeit von 23andMe:

23andMe nutzt ein Verfahren der Genotypisierung, bei dem nur bestimmte Stellen des Genoms analysiert werden, von denen das Unternehmen durch wissenschaftliche Untersuchungen zu wissen meint, dass sie Einfluss auf Ihre Gesundheit oder Ihre Abstammung haben. Eine komplette Analyse würde eine Entschlüsselung der kompletten DNA nötig machen, was derzeit zu diesem Preis nicht möglich ist. 23andMe analysiert etwa eine Million individuelle Stellen von den drei Milliarden Basenpaare des kompletten Genoms, also etwa ein halbes Prozent. Alle menschlichen Wesen teilen sich rund 99,5 Prozent ihrer gesamten DNA, 23andMe hat es bei der Untersuchung auf die Unterschiede abgesehen.

23andMe verfolgt keinen medizinischen Ansatz, also vorrangig diejenigen Gene anzusehen, die für eine bestimmte Erkrankung in Frage kommen. Vielmehr sollen „so viele Daten wie nur irgend möglich“ gescannt werden, um zu erkennen, „was deine DNA sonst noch über dich verrät“. Für seine KundInnen erstellt 23andMe einen sogenannten Krankheitsreport, der Hinweise darauf geben soll, wie groß die Wahrscheinlichkeit ist, an bestimmten Leiden zu erkranken. Derzeit sind es 250 Aussagen, die „nach dem heutigen Stand der Forschung“ getätigt werden. Von der Analyse erfasst werden etwa 50 unterschiedliche Erbkrankheiten, wie zum Beispiel Mukoviszidose. Daneben gibt es einen allgemeinen Krankheitsreport, der prognostizierte Wahrscheinlichkeiten für unterschiedliche Erkrankungen benennt. Andere Berichte geben Aufschluss darüber, welche Wirkstoffe man verträgt und wie der Körper diese annimmt. Zudem gibt es einige allgemeine Angaben über die Physiognomie.

23andMe verspricht, seine KundInnen über medizinische Errungenschaften auf dem Laufenden zu halten. Dessen Expertenteam aktualisiere auf der Basis des aktuellen Stands der Forschung die Gesundheits-Reports ständig und liefere den Betroffenen somit eine Art Update. 23andMe konnte im November 2007 gerade einmal 14 individuelle Aussagen treffen – zu einem Preis von 999 Dollar. 2013 werden für den Preis auf 99 Dollar 250 unterschiedliche Analysepunkte benannt.

Das Unternehmen analysiert so viel von dem Genom wie möglich in der Hoffnung und dem Vertrauen darauf, dass die Daten eines Tages mit dem Fortschritt der Wissenschaft wertvoll werden. Ende 2013 hatte 23andMe mehr als 450.000 genotypisierte KundInnen; das Ziel ist es viele Millionen Proben zu erhalten: „Je mehr Daten wir haben, desto besser sind wir in der Lage, genetische Entdeckungen zu machen. Letztendlich ist unser Ziel, neue Heil- und Behandlungsmethoden zu finden. Big Data macht das möglich.“

23andMe hat sich in den ersten fünf Jahren vor allem darauf konzentriert, eine solide wissenschaftliche Grundla-

ge für seine Forschungsarbeit zu schaffen. Danach ist das Unternehmen dazu übergegangen, seinen Schwerpunkt auf Wachstum und Masse zu verlagern, weshalb der Preis immer weiter abgesenkt wurde. Ende 2012 hatte eine Analyse noch 299 Dollar gekostet; nun sind es 99 Dollar. Dies war möglich, nachdem Dezember 2012 Yuri Milner, ein russischer Investor, 15 Millionen Dollar Risikokapital in das Unternehmen steckte. „Wenn man erst einmal die Daten von einer Million Menschen hat, ist die Schlagkraft, die man dadurch erlangt, gewaltig. Es gibt zahlreiche Möglichkeiten, unsere Forschung und die Daten, die wir besitzen, zu monetarisieren. Da wird es sicherlich noch Möglichkeiten geben, die wir heute noch gar nicht antizipieren können. Das hängt alles von den Daten ab. Wir werden über die Jahre sicherlich neue Verwertungswege und Angebote schaffen.“

Datenschutz

Das Unternehmen gibt an, die Kundendaten gut zu schützen, zumal „man im DNA-Gewerbe ohne Vertrauen kein Geschäft machen kann“. Da das Unternehmen aber ein Online-Anbieter ist, bleiben aus Sicht des Unternehmens „gewisse Risiken“. Die Gen-Daten und die persönlichen Daten der KundInnen werden an zwei unterschiedlichen Orten gespeichert. Erst wenn sich eine KundIn auf ihrem Konto einloggt, würden diese Datensätze zusammengeführt. Für die Forschung gäbe es einen separaten Bereich; ungefähr 90% entscheiden sich für eine Teilnahme an dem Programm, das dem Unternehmen die Möglichkeit eröffnet, mit den genetischen Daten wissenschaftliche Analysen durchzuführen. Die Forschenden haben nach Firmenangaben keine Möglichkeit, Namen, Wohnadressen, Kreditkarteninformationen oder dergleichen einzusehen: diese Daten seien in einer separaten Datei gespeichert. Wo in den USA die Gen-Daten gespeichert sind, sagt das Unternehmen „aus Sicherheitsgründen“ nicht.

Zu den Datenschutzbedenken vieler Menschen meinte Catherine Afarian: „Viele Menschen machen sich Sorgen, weil wir es bei der Genetik mit einem Forschungsfeld zu tun haben, das noch in den Kinderschuhen steckt. Wer weiß schon, was in fünf oder vielleicht zehn Jahren alles möglich sein wird. Ich denke, dieser Gedanke macht die Menschen vorsichtig. Du triffst heute eine Entscheidung, aber du hast keine Ahnung, welche Konsequenzen das möglicherweise in der Zukunft hat. Für einen Hacker sind Kreditkarten-Informationen heutzutage vermutlich wertvoller als genetische Fingerabdrücke. Aber gilt das auch noch in der Zukunft? Menschen hängen sehr an ihrem Geld, aber ich glaube, sie machen sich noch mehr Sorgen um ihre Gene. Weil es sprichwörtlich ein Teil von ihnen ist. Es handelt sich eben nicht nur um Einsen und Nullen, die man völlig losgelöst von sich selbst betrachten kann. Es handelt sich um das Rezept, das uns zu dem macht, der wir sind. Darum wird es auch oft emotional, wenn das Thema Genetik und Datenschutz diskutiert wird. Das ist menschlich.“

Forschungsbasis

Das Unternehmen will Dritten im Rahmen seines Geschäftsmodells auf keinen Fall den Zugang zu den Daten einräumen: „Sämtliche Forschungsarbeiten werden von unseren eigenen Mitarbeitern erledigt.“ Durch die Datenmenge könne Effizienz in den Forschungsprozess gebracht werden: „Nehmen wir zum Beispiel Parkinson. Ein Wissenschaftler würde Jahre damit verbringen, Ärzte zu finden, die bereit sind, an Parkinson Erkrankte für eine Studie zu gewinnen. Dann benötigen Sie eine Kontrollgruppe. Bis Sie die Ergebnisse Ihrer Forschung publiziert haben, sind ohne weiteres sechs bis acht Jahre ins Land gegangen. Wir bei 23andMe haben schon heute mehr als 10.000 von Parkinson Betroffene als Teil unseres Research-Programms – das ist die größte Gen-Datenbank von Parkinson-Patienten weltweit. Unsere ersten Studien, die wir zu dem Thema veröffentlicht haben, wurden in weniger als 18 Monaten erstellt. Wir können uns auf völlig neue Gebiete konzentrieren. Zum Beispiel auf die Frage, ob es neben den Genen noch weitere Faktoren gibt, die Einfluss auf bestimmte Krankheiten haben. Ist es gar das Verhalten?“

Über Fragebögen versucht 23andMe, weitere Erkenntnisse über seine KundInnen zu erlangen, über das, „was Sie tun, was Sie nicht tun, wie Ihre Krankheitsgeschichte aussieht“. Aus diesen Daten sollen auffällige Verhaltensmuster abgeleitet werden, die Auswirkungen auf die Gesundheit haben können: „Die Kombination, dass wir sowohl Umwelteinflüsse als auch die Gen-Daten sammeln, ist unschlagbar.“

Diskriminierung oder Prävention

In den Vereinigten Staaten gibt es seit 2008 ein Bundesgesetz, den Genetic Information Nondiscrimination Act. Dieses Gesetz verbietet es Arbeitgebern und Krankenkassen, Menschen aufgrund ihrer Gen-Informationen zu diskriminieren. Allerdings sind Ausnahmen vorgesehen, z. B. für langfristige Pflege-Policen. Zudem ist möglich, dass Versicherungen Bonus-Programme anbieten für Menschen, die ihre DNA freiwillig zur Verfügung stellen.

Für Afarian ist „die richtige Vorsorge“ ein möglicher Ansatz: „Unsere Mission als Firma ist es, das Gesundheitswesen dahin zu bewegen, Krankheiten nicht erst zu bekämpfen, wenn sie schon eingetreten sind. Man möchte doch erst gar nicht krank werden! Es gibt zahlreiche Studien, die belegen, dass richtige Vorsorge unglaublich effektiv sein kann. Wir wissen beispielsweise, dass gewisse Krankheiten in bestimmten Bevölkerungsgruppen häufiger auftreten als in anderen. Sichelzellenanämie ist eine Erkrankung, die vor allem bei Afroamerikanern verbreitet ist. Mukoviszidose hingegen tritt häufiger bei Aschkenasi-Juden auf. Solche Krankheiten lassen sich zwar sicherlich nicht allein durch Vorsorge verhindern, aber wenn man weiß, man hat irgendwo eine mögliche Schwäche, dann kann man beizeiten besser darauf achtgeben. Es gibt Stimmen, die glauben, es ist nur eine Frage der Zeit, bis die Genotypisierung des Menschen zum Standard wird, schon bei der Geburt“.

Reaktionen

Der Aachener Humangenetiker Klaus Zerres meint zu dem Angebot von 23andMe: „Diese Tests sind nicht seriös.“ Er und andere Experten in Deutschland, wie z. B Claus Bartram von der Uni

Heildelberg oder sein Bonner Kollege Peter Propping, begrüßen, dass die FDA dem Unternehmen weitere DNA-Tests untersagt (Gutjahr, Sie haben ein erhöhtes Risiko für Prostata-Krebs, www.faz.net 07.11.2013; US-Behörde stoppt Gentest-Frma 23andMe, www.heise.de 26.11.2013; Blawat, Ausgespuckt, SZ 27.11.2013, 1).

USA

Kein Persönlichkeitsrecht für Tiere

TierschützerInnen in den USA scheiterten bei ihrem Versuch, Persönlichkeitsrechte von Schimpansen gerichtlich anerkennen zu lassen. Drei Gerichte im US-Bundesstaat New York wiesen Klagen ab, mit denen die Vereinigung „Nonhuman Rights Project" ein „Recht auf körperliche Freiheit" für vier Affen durchsetzen wollte. Die KlägerInnen kündigten Beschwerde vor der nächsten Instanz an. Der Präsident der Vereinigung, Steven Wise, sagte, die Richter sollten erstmals anerkennen, dass „kognitiv komplexe, selbstständige Lebewesen" das Grundrecht besäßen, nicht in Gefangenschaft gehalten zu werden. Aufgehängt war die Klage an den Schimpansen Tommy, Kiko, Hercules und Leo, die bei unterschiedlichen Haltern als Haustiere leben. Die Tierrechte-Vereinigung teilte mit, weitere Klagen für Tiere einreichen zu wollen, die „wissenschaftlich erwiesen Selbstbewusstsein besitzen und selbstbestimmt sind". Dazu zählten auch Elefanten, Delfine und Wale (Gericht: Affen haben kein Persönlichkeitsrecht, SZ 11.12.2013, 9).

Kanada

CSEC bespitzelt Fluggäste für NSA

Der kanadische Geheimdienst Communications Security Establishment Canada (CSEC) hat im Auftrag der US-Regierung Passagiere an Flughäfen ausspioniert. Medien berichteten unter Berufung auf Dokumente des ehemaligen US-Geheimdienstmitarbeiters Edward Snowden, dass der CSEC die Daten von Fluggästen abgegriffen hat, die sich mit ihren mobilen Geräten in Drahtlosnetzwerke eingeloggt hatten. Über Verbindungen zu anderen öffentlichen Netzwerken in Cafés, Hotels oder Bibliotheken habe der Geheimdienst anschließend das Bewegungsprofil der Betroffenen in Kanada und an US-Flughäfen über Tage verfolgen können. Die Abhöraktion sei ein Test für eine nun einsatzfähige Software gewesen, die gemeinsam mit dem US-Geheimdienst NSA entwickelt worden sei. Kanadische Gesetze sehen vor, dass das CSEC auf kanadischem Boden niemanden ohne Genehmigung ausforschen darf (Fluggäste ausspioniert, newsticker.sueddeutsche.de 01.02.2014).

Australien

Lauschangriff auf indonesische Regierung

Der indonesische Präsident Susilo Bambang Yudhoyono ist Medienberichten zufolge Ziel eines australischen Lauschangriffs geworden. Der Nachrichtendienst DSD habe versucht, Handy-Telefonate des Staatsoberhaupts mitzuhören. Gut zwei Wochen lang wurden Uhrzeit, Gesprächsdauer und Rufnummern der Gesprächspartner registriert, die der indonesische Präsident kontaktierte. Ein Mithören der Gespräche sei gescheitert. Dies wurde unter Berufung auf Dokumente von NSA-Aufdecker Edward Snowden berichtet. Gemäß den Unterlagen aus dem Jahr 2009 nahmen die Spione auch Yudhoyonos Frau und hochrangige Regierungsmitglieder ins Visier. Das australische Außenministerium und das indonesische Präsidialamt lehnten zunächst eine Stellungnahme zu den Berichten ab. Der indonesische Außenminister Marty Natalegawa rief am 18.11.2013 seinen Botschafter in der australischen Hauptstadt Canberra zu Konsutationen zurück: „Ich kann gar nicht deutlich genug machen, wie ernst wir diese Sache nehmen". Die Berichte könnten die Beziehungen der beiden Staaten zusätzlich belasten. Oktober 2013 hatten Medien berichtet, dass australische Botschaften quer durch Asien, darunter auch in Indonesien, eine Rolle bei einem von den USA geleiteten elektronischen Überwachungseinsatz spielen (Präsident ausspioniert, SZ 19.11.2013, 8; Australischer Lauschangriff auf Indonesien, www.salzburg.com 18.11.2013).

Südkorea:

20 Mio. Bankdatensätze gestohlen

Eine Sprecherin des südkoreanischen Finanz-Aufsichtsdienstes FSS teilte am 20.01.2014 mit, dass über ein riesiges Datenleck bei südkoreanischen Banken und Kreditkartenfirmen vertrauliche Informationen von etwa 20 Millionen KundInnen in falsche Hände geraten sind. Es seien mehr als 20 Verdächtige festgenommen worden, darunter ein Mitarbeiter der Kreditratingfirma Korea-Kreditbüro (KCB). Unter den Festgenommen sollen sich auch Personen aus dem Kreis privater Kreditgeber und Werbeunternehmen befinden. Premierminister Chung Hong Won wies den FSS zu einer gründlichen Untersuchung an. Die Behörden vermuten, dass die Datensätze verkauft werden sollten. Die Datensätze enthalten Konto- und Meldenummern sowie Informationen zur Kreditwürdigkeit der Betroffenen. Die Aufsichtsbehörde FSS ging zunächst nicht von einem weiteren kriminellen Missbrauch aus: „Die Wahrscheinlichkeit, dass die Kreditkarten kopiert werden, ist sehr gering, weil keine Passwörter oder Kartenprüfnummern gestohlen wurden." Die drei großen Kreditkartenfirmen des Landes, KB Kookmin Card, Lotte Card und Nonghyup, die ihre Kundendaten mit den verbundenen Banken teilen, entschuldigten sich für den Datenklau (20 Millionen Daten weg, SZ 21.01.2014, 14).

Arabische Staaten

Homosexuelle mit „medizinischen Tests" aufspüren?

Ein kuwaitischer Politiker will mit medizinischen Tests Schwule entlarven - und sie an der Einreise nach Kuwait und andere Golfstaaten hindern. Wie der Test aussehen soll, verriet

der Politiker nicht. Medizinische Tests für AusländerInnen sind im arabischen Raum keine Seltenheit. Wer in Ländern der Golfregion oder auch in Syrien länger arbeiten oder studieren will, muss zu Beginn einen Gesundheitstest absolvieren. Das ist für gewöhnlich eine rasche Routineuntersuchung und ein Aids-Test. Yussuf Mindkar, Direktor für öffentliche Gesundheit im kuwaitischen Gesundheitsministerium, reicht das jedoch nicht und fordert einen Test, der Homosexuelle „entdeckt,“: „Wir müssen strengere Maßnahmen ergreifen, die uns helfen, Schwule zu entlarven, die wir dann an der Einreise nach Kuwait oder andere GGC-Staaten hindern können.“

Im Golf-Kooperationsrat (GCC) sitzen neben Kuwait auch Bahrain, Katar, Oman, Saudi-Arabien und die Vereinigten Arabischen Emirate. In allen Staaten ist Homosexualität verboten, die meisten ahnden ein Vergehen mit langjährigen Haftstrafen; Saudi-Arabien bestraft gleichgeschlechtliche Liebe gar mit der Todesstrafe. Mindkar stellte seinen Vorschlag für härtere Tests bei einem GCC-Treffen am 11.11.2013 offiziell vor. Sollte der Vorschlag durchkommen, könnte die Schwulen-Grenzkontrolle auch im WM-Austragungsland Katar eingeführt werden. Homosexuellenrechtler forderten den Weltfußballverband Fifa auf, die WM in Katar zu stoppen. Katar könnte so ähnlich in die Schusslinie geraten wie derzeit Russland. Wie genau sich Mindkar diese Tests vorstellt, sagte er nicht. „Al Rai“ zitiert ihn lediglich mit der Idee, in Gesundheitszentren klinische Untersuchungen einzuführen, die „Homosexuelle offenbaren“ und ihnen eine Art Zertifikat auszustellen, auf dem „nicht anständig/ nicht gemäß“ vermerkt ist. Solch ein Test könnte auf - wie in Nordafrika üblich - Analuntersuchungen oder auch auf Phallografie basieren. Dabei wird der Blutdruck im Penis bei sexueller Erregung gemessen. Phallografien werden unter anderem an Asylbewerbern in Tschechien durchgeführt (DANA 1/2012, 24 f.).

Erst im Mai 2013 hatten kuwaitische Polizisten 215 Schwule und Lesben in einer groß angelegten Razzia in mehreren Internetcafés festgenommen. Und im Jahr 2010 wurde die Ausstrahlung eines ägyptischen Films („Bidun Rakaba“ - Ohne Kontrolle) verhindert, der neben Drogengebrauch auch Homosexualität thematisierte. In 78 Ländern, darunter fast allen arabischen Staaten, ist Homosexualität verboten, in Saudi-Arabien, Iran, Sudan, Jemen und Mauretanien gilt die Todesstrafe. Amnesty International nannte die Pläne der Golf-Staaten „unerhört“. Solche Empörungen sind zugleich eine Steilvorlage für bärtige Frömmler, die damit sowohl ihren Ekel vor den „Ausschweifungen“ des Westens wie auch ihre patriotische Gesinnung unter Beweis stellen können (Röhlig, Kuwait will Homosexuelle an Einreise hindern, www.tagesspiegel.de 10.11.2013; Zekri, Moral und Verbrechen, SZ 16.10.2013, 9).

Technik-Nachrichten

Atemanalysen - nicht nur zur medizinischen Diagnostik

Aussagekräftiger Duft

Schon der griechische Arzt Hippokrates von Kos wusste vor gut 2500 Jahren, dass man Krankheit riechen kann. Er bat seine PatientInnen, ihn einmal kräftig anzuhauchen, woraus der dann seine Schlüsse zog. Heilpraktiker, die nach der traditionellen chinesischen Medizin arbeiten, schließen u. a. aus dem Geruch des Atems auf mögliche Beschwerden. Auch in der westlichen Medizin weiß man längst, dass Krankheiten ihre olfaktorischen Spuren hinterlassen. DiabetikerInnen verströmen oft einen leichten Geruch nach Nagellackentferner bzw. dessen Inhaltsstoff Aceton, der sich bildet, wenn eine Unterversorgung mit Zucker vorliegt. Eine kranke Leber, die gewisse Stoffwechselprodukte nicht mehr abbaut, lässt die PatientInnen nach tierischer Leber und Erde riechen; Nierenkranke sind an einem Hauch von Ammoniak erkennbar. Wenn ein Mensch verlockend nach frischem Brot duftet, kann das auf Typhus hindeuten. Schon vor Jahren haben amerikanische Forschende von der Pine-Street-Stiftung im kalifornischen San Anselmo gezeigt, dass trainierte Hunde an menschlichen Atemproben erschnüffeln konnten, ob der Probengeber an Brust- oder Lungenkrebs erkrankt war oder nicht.

Die medizinische Atemanalyse hat also Potenzial, in das diagnostische Arsenal der Schulmedizin aufgenommen zu werden, wenn elektronische Nasen die fehleranfälligen Riechorgane von Mensch und Hund ersetzen und eine breite Datenbasis es erlaubt, die gewonnenen Ergebnisse richtig zu deuten.

Die Funktionsweise

Es sind sog. Metabolite, die in der Atemluft gemessen werden und MedizinerInnen und WissenschaftlerInnen Hinweise auf vorhandene Erkrankungen geben sollen. Diese Moleküle sind Zwischenprodukte, die bei biochemischen Stoffwechselvorgängen entstehen. Manche Metabolite deuten auf spezifische Vorgänge hin, die typisch für einzelne Krankheiten sind. Jan Baumbach, Bioinformatiker an der Universität Süddänemark in Odense, forscht an neuen Methoden zur entsprechenden Datenauswertung: „Wichtig ist es herauszufinden, welche Kombinationen von Metaboliten Rückschlüsse auf welche Krankheiten erlauben, da ist die Datenlage einfach noch viel zu dünn.“ Technisch sei inzwischen viel möglich. Es gibt drei unterschiedliche Methoden, um den Atem von Patienten zu analysieren: Sensortechniken, die Ionenbeweglich-

keitsspektrometrie und die Massenspektromie.

Baumbach hatte zuvor im Exzellenzcluster „Multimodal Computing and Interaction“ an der Universität des Saarlandes gemeinsam mit dem Korea Institute for Science and Technology Europe (KIST Europe) Proben von Ärzten aus zahlreichen medizinischen Einrichtungen, unter anderem in Hemer, Homburg, Essen, Göttingen und Marburg analysiert. Die Ärzte hatten im Rahmen von klinischen Studien die Ausatemluft von PatientInnen mit bekannten Erkrankungen untersucht. Die BioinformatikerInnen der Universität Saarbrücken prognostizierten, dass die entwickelten Computer-Algorithmen für die Auswertung von Atemanalysen in wenigen Jahren in zusätzliche Hardware von Smartphones eingebaut werden könne, um dann beispielsweise Bakterien und Tumore schneller und zuverlässiger zu bestimmen oder den Blutzuckergehalt per Pusten ins Smartphone zu überprüfen.

Die preisgünstigsten Geräte kosten 2013 noch 10.000 Euro und arbeiten mit der Sensortechnik, sie eignen sich allerdings nur, wenn man genau weiß, wonach man sucht und möglichst nichts oder nur wenig anderes da ist. Dies ist bei Atemluft regelmäßig schwierig. Jörg Baumbach, der lange am ISAS, dem Leibniz-Institut für analytische Wissenschaften an der Technischen Universität Dortmund an Hardware zur Atemanalyse forschte und 2009 mit den Ergebnissen das Unternehmen B&S Analytik gründete, beschäftigt sich im Sonderforschungsbereich 876 der Deutschen Forschungsgemeinschaft mit der Frage, wie Spektrometer beschaffen sein müssen, um eine optimale Atemprobe vom PatientInnen zu nehmen und diese exakt und ohne verfälschende Einflüsse zu deuten: „Für komplexe Gemische eignet sich die Ionen-Mobilitäts-Spektrometrie besonders gut, damit sind derzeit mehr als 600 Metabolite messbar und die Geräte sind so beweglich, dass sie auch am Patientenbett einsetzbar sind.“ Diese Geräte kosten von 50.000 Euro an aufwärts. Am weitaus besten lassen sich die im Atem enthaltenen Stoffe mit dem Massenspektrometer quantifizieren und identifizieren. Die Geräte sind jedoch mit mehr als 120.000 Euro extrem teuer und sehr immobil. Damit sind sie hervorragend geeignet für Analysen im Labor, aber kaum direkt bei PatientInnen einsetzbar.

Mit der Atemanalyse ist es grundsätzlich möglich, eine Art Fingerabdruck des Atems zu erstellen und herauszufiltern, welche Bestandteile in der Ausatemluft normal oder ungefährlich sind und welche auf eine therapiebedürftige Erkrankung hindeuten. Medikamente zum Beispiel, die ein Mensch nehmen muss, werden abgebaut und hinterlassen genauso ihre Spuren wie eine harmlose Infektion oder Erkältung. Hinzu kommt, dass sich der Atem eines jeden Menschen im Tagesverlauf immer wieder unterschiedlich zusammensetzt. Jan Baumbach erläutert: „Sie müssen sich vorstellen, dass wir beim Atmen wirklich alles aufnehmen und dann entsprechend auch messen - vom Parfum der Krankenschwester, die die Untersuchung durchführt, über das, was der Patient zu Mittag gegessen hat, bis zu den Abbauprodukten des frisch gemähten Rasens, über den er kurz vor der Untersuchung gelaufen ist. Unsere Nachweisgrenze ist deutlich höher als die einer Hundenase.“

Aus vielen individuellen Merkmalen muss eine Basis geschaffen werden, aus der allgemeingültige Kriterien für die Diagnose von Krankheiten gewonnen werden können. Um eine weltweit verfügbare Datenbank speisen zu können, sind viele Atemproben - von Gesunden und Kranken, Alten und Jungen, Männern und Frauen, morgens, mittags, abends und nachts genommen - nötig. Jan Baumbach: „Leider stehen wir da immer noch vor einer Anwendungsbarriere. Viele Mediziner lassen sich ungern von einer Maschine erzählen, was ihre Patienten haben könnten.“ Doch je mehr Erfolge mit der Atemanalyse publiziert werden, umso mehr schmelze auch der Widerstand. Abgesehen von den erzielbaren Resultaten punktet die Diagnose durch Duftmoleküle auch durch ihre pragmatische Seite: Sie ist schnell, billig und nicht invasiv. Gewebeproben, Röntgen, ja selbst das Blutabnehmen bergen für die PatientInnen mehr Risiken und sind mit mehr Aufwand verbunden als das Ausatmen. Selbst bei Bewusstlosen kann der Atem überprüft werden. Die medizinische Atemanalyse hat also durchaus das Zeug dazu, ins diagnostische Arsenal der Schulmedizin aufgenommen zu werden.

Individueller Atemabdruck

Forschende an der ETH Zürich und dem Universitätsspital Zürich verfolgen auch das Ziel einer objektiven Atemanalyse. Renato Zenobi, Professor am Laboratorium für Organische Chemie, und seine Kollegen nutzen ein Massenspektrometer, mit dem das Molekulargewicht von Substanzen gemessen werden kann. In einer Studie, die im April 2013 im Fachmagazin Plos One erschienen ist, haben die Schweizer den Atem von elf Versuchspersonen über elf Tage lang gemessen. Zwar schwankten die Profile der Teilnehmenden je nach Tag und Tageszeit. Doch mit statistischen Verfahren erstellten die WissenschaftlerInnen individuelle Atemabdrücke. Die Zuordnungswahrscheinlichkeit lag angesichts des kurzen Erhebungszeitraumes im Mittel bei 76 %. Mit etwa 30 Atemspektren eines Menschen lasse sich, so die Prognose, der Atemabdruck zu 100 % zuverlässig zuordnen. Die Studie richtete sich nicht auf die Bestimmung einzelner Inhaltsstoffe wie etwa Aceton oder Acetaldehyd, sondern lediglich auf das Profil des gesamten Atemabdrucks. Zenobi: „Wir sprechen da von einer sogenannten Kernsignatur, die trotz geringer tageszeitlicher Schwankungen konstant genug ist, dass sie für die medizinische Anwendung brauchbar ist.“ Die Technik sei aber noch nicht massentauglich.

Nachdem man weiß, dass jeder Mensch einen individuellen Atemabdruck habe, gehe es darum, diesen über einen längeren Zeitraum zu verfolgen und zudem die entsprechende Signatur von Krankheiten zu entschlüsseln, den sogenannten Breathprint. Dafür wird der Atem von PatientInnen verglichen, die alle die gleiche Lungenkrankheit haben. Die Forschenden hoffen, Muster zu entdecken, die sich bei allen Kranken findet, um so eine Diagnosemöglichkeit entwickeln zu können. Bei Atemkrankheiten rechnen sie sich die höchsten Chancen auf einen raschen Fund bestimmter Biomarker aus. Langfristig sollen jedoch auch die Signaturen anderer Krankheiten identifiziert werden können. Die Analyse ist aber kein Allzweckmittel: „Ich bin mir sicher, dass wir nicht all das, was wir über Blut und Urin analysieren können, im Atem besser repräsentiert haben. Aber die Atem-

analyse hat den entscheidenden Vorteil, dass sie unheimlich schnell ist.“

Wegen dieser Unmittelbarkeit eröffnet die Atemanalyse vielleicht sogar neue Möglichkeiten, die Therapien von Schwerkranken zu verbessern. Im Falle einer Sepsis zum Beispiel, in der Ärzte gegen die Zeit kämpfen, könnte innerhalb von ein, zwei Stunden getestet werden, ob das eingesetzte Antibiotikum wirkt oder auf ein anderes Mittel ausgewichen werden muss. Ähnlich könnte die Atemanalyse während einer Chemotherapie eingesetzt werden - kommen die ausgewählten Medikamente auch wirklich ihrer zugedachten Aufgabe nach oder muss vielleicht die Dosierung verändert werden? Jan Baumbach, der in der Früherkennung von Krankheiten ein weiteres großes Potenzial der Atemanalyse sieht: „Das wird sicher noch eine Weile dauern, bis das in der alltäglichen Praxis so umsetzbar ist, aber wir sind da dran“. Beim Hausarzt könnte dann zum routinemäßigen Blutdruckmessen auch die routinemäßige Atemanalyse kommen. Binnen kürzester Zeit wüsste der Mediziner, ob seine PatientIn Hinweise auf eine Krankheit in sich trägt, die behandelt werden muss - das therapeutische Fenster könnte sich dadurch deutlich nach vorne schieben lassen.

Alltagsanwendungen

Die Technologie muss aber nicht nur im medizinischen Bereich eingesetzt werden: Forschende der Universität von Cardiff/Wales veröffentlichten schon im Jahr 2008 im Magazin „New Scientist“, wie damit der Heimweg ganzer Massen von Betrunkenen sicherer gemacht werden könne. Durch das Studium der nächtlichen Bewegung von Menschenmassen im Zentrum von Cardiff, wo Nachtschwärmenden etliche Pubs und Bars bevölkern, beobachteten die Forscher insgesamt 24-mal zwischen 23 Uhr und 3 Uhr die Heimwege von Menschenmassen. Sie machten Atemanalysen, um den Grad der Trunkenheit festzustellen, und zeichneten die Gangart und Wege der Kneipenbesucher auf. Mit den Daten fütterten die WissenschaftlerInnen um Simon Moore ein Computermodell des Verhaltens von Menschenmassen, um hieraus präventive und repressive Konzepte ableiten zu können. Nicht ganz unerwartet fanden die Forschenden heraus, dass Menschengruppen sich umso langsamer und großflächiger fortbewegen, je mehr Betrunkene mitlaufen. Verbesserte Atemanalysen sind auch eine Grundlage für schnelle Alkoholkontrollen im Straßenverkehr, mit denen nicht nur der Alkoholgehalt der Atemluft, sondern mit dem das individuelle Atemprofil und damit die Identität der Kontrollierten festgehalten werden kann (Füssler, Schnüffel-Diagnose, SZ 24.10.2013, 14; Atem lässt sich für Krankheits-Diagnose nutzen, www.welt.de 08.04.2013; Atemanalyse bald über Smartphone? www.curado 16.04.2012, Früherkennung von Krankheiten über Atemanalysen rückt näher, www.aerzteblatt.de 07.03.2012; Forscher wollen Straßen sicherer für Betrunkene machen, www.t-online.de 24.07.2008).

Amazon: Warenkorbanalyse verkürzt Lieferzeiten

Amazon wurde ein Patent zugesprochen, das dafür sorgen soll, dass ein Produkt schon auf dem Weg zum Kunden ist, bevor dieser seine Wahl getroffen und den Button „Kaufen“ angeklickt hat. Beim „vorausschauenden Versand“ („anticipatory shipping“) werden bestimmte Waren schon einmal an ein Versandzentrum geschickt, in dessen Nähe sich ein oder mehrere Kunden höchstwahrscheinlich für das Produkt interessieren. Wird es dann schließlich bestellt, ist es schneller beim Empfänger. Ausgewertet werden hierfür frühere Bestellungen, Umtäusche, Wunschzettel bei Amazon, der Inhalt der Einkaufswagen - und sogar, wie lange ein Kunde mit dem Mauszeiger auf einer Produktbeschreibung verweilt.

Amazon versucht schon seit langem seine Lieferzeiten zu optimieren. Wer online einkauft, muss immer eine Weile warten, bis er das Produkt in der Hand hält. Je kürzer diese Weile ist, umso niedriger ist das Risiko für den Versandriesen, dass die Kunden in ein normales Geschäft um die Ecke gehen, um einzukaufen. Im Dezember 2013 hatte Amazon bekanntgegeben, mit Mini-Drohnen zu experimentieren, um die Lieferzeit zu verkürzen. Laut Firmenchef Jeff Bezos sollen es die unbemannten Flugobjekte möglich machen, bestellte Ware binnen 30 Minuten vom Versandzentrum bis zum Kunden zu transportieren (Amazon will schon vor der Bestellung liefern, www.spiegel.de 18.01.2014).

Passworterkennung per Analyse von Computergeräuschen

Mit Hilfe von kaum hörbaren Geräuschen, die Computer von sich geben, haben israelische Forschende eine als ziemlich sicher geltende Verschlüsselung ausgehebelt. Computer erzeugen während des Betriebs eine Vielzahl von Geräuschen, etwa vom Lüfter oder vom DVD-Laufwerk. Die kaum hörbaren und für Menschen nicht identifizierbaren Geräusche von Computerchips können offensichtlich Daten über die laufenden Programme enthüllen. Mit einem Mikrofon haben israelische Informatiker nun Passwörter für die E-Mail-Verschlüsselung durch eine sogenannte akustische Kryptoanalyse der typischen Muster von Rechenoperationen berechnet. Die Informatiker Daniel Genkin, Adi Shamir und Eran Tromer von der Tel Aviv University in Israel konnten aus den Geräuschen der laufenden Verschlüsselungssoftware GnuPG, einer freien Version des bekannten PGP-Verschlüsselungsprogramms, den privaten Schlüssel extrahieren. Dieser wird eingesetzt, um in dem Verfahren eine für einen bestimmten Empfänger gedachte Nachricht zu dekodieren. Die Verschlüsselung der Nachricht läuft hingegen über einen öffentlichen Schlüssel. So kann zwar jede Person Nachrichten verschlüsseln und an den Empfänger senden, aber nur dieser ist in der Lage, sie zu lesen.

Die Forscher um Shamir, den Miterfinder und -namensgeber des kryptografischen RSA-Verfahrens, haben für ein jüngst veröffentlichtes Papier gezeigt, dass sie innerhalb einer Stunde einen solchen Schlüssel herausfinden und damit knacken konnten. Dafür versandten sie Nachrichten an einen Versuchslaptop. Der Inhalt dieser Nachrichten war ihnen bekannt. Sobald das E-Mail-Programm des Empfängerrechners diese Nachrichten entschlüsselte, gaben die

dabei erzeugten Töne Aufschluss über den Schlüssel selbst. Mit immer neuen und abgeänderten Nachrichten ließ sich Bit für Bit herausfinden, mit was für einem privaten Schlüssel die Nachrichten in einen lesbaren Text zurückverwandelt wurden. Gemäß den Forscherangaben wäre ein einfaches Mobiltelefon neben dem Rechner ausreichend, um solche Attacken auszuführen. Über platzierte Wanzen ließen sich aus der Ferne Tonanalysen durchführen. Nur das Audiosignal wird dafür benötigt. So zeigten die Informatiker auch, dass ein Richtmikrofon und eine aktenkoffergroße Messstation aus vier Metern Entfernung geeignet ist, um die Geräusche des Rechners mit ausreichender Qualität aufzuzeichnen. Die Attacke sei zudem bei mehreren verschiedenen Rechnermodellen erfolgreich gewesen.

Gemäß den Angaben der Forscher ist auch die elektrische Spannung, unter der ein Laptop-Gehäuse steht, für eine Kryptoanalyse nutzbar. Durch Berührung des Computers oder eine zusätzliche Leitung am USB- oder Bildschirm-Kabel sind Spannungsschwankungen einfach übertragbar und leicht auszuwerten. Sie lassen sich ähnlich einsetzen, um den Schlüssel Stück für Stück zu rekonstruieren. Um diese Ausspähmethoden für die als sicher geltende E-Mail-Verschlüsselung PGP zu unterbinden, haben die Forscher die Sicherheitslücke erst zusammen mit einem Update der Software veröffentlicht, mit dem das Problem beseitigt werden soll. Nutzer des Verschlüsselungsprogramm GnuPG in den Versionen 1.x sollten ihre Programme umgehend aktualisieren. Vor allem, falls sie davon ausgehen müssen, dass die Tonsignale ihrer Rechner leicht aufzuzeichnen sind. Nutzer der modernen Varianten der Software sind nicht von dem Problem betroffen (Forscher knacken Passwort über Computergeräusche, www.spiegel.de 20.12.2013).

Pupille spiegelt Gesichtsbild von Angreifer

Entführer oder Sexualverbrecher fotografieren häufig ihre Opfer. Dies könnte künftig zu ihrer Überführung beitragen, weil sie sich dabei möglicherweise selbst fotografieren, denn in den Pupillen der Opfer lässt sich bei hochaufgelösten Digitalbildern das Konterfei des Täters erkennen. Psychologen von der University of York und der University of Glasgow haben nachgewiesen, dass solche durch 30.000fache Vergrößerung sichtbar gemachten Spiegelbilder von der Pupille meist korrekt dem entsprechenden Passfoto einer Person zugeordnet werden können. Wenn die Testteilnehmenden die Dargestellten nicht kannten, wählten sie in 71% der Fälle das zur Vergrößerung passende Bild; bei vertrauten Gesichtern stieg die Trefferquote auf 84%. Studienleiter Rob Jenkins erklärte: „Die Pupille ist wie ein schwarzer Spiegel. Um das darin enthaltene Bild zu vergrößern, muss man hineinzoomen und die Kontraste erhöhen.“ Die menschliche Fähigkeit zur Gesichtserkennung funktioniere offenbar auch bei sehr verpixelten Aufnahmen. Die Forschenden hoffen, dass bei Ermittlungen mit solchen Spiegelbildern - etwa aus Kinderpornofotos im Internet - Täternetzwerke rekonstruiert oder die Anwesenheiten von Personen an bestimmten Orten belegt werden können (Der Spiegel 2/2014, 114).

Ixquick/StartPage verzeichnen im Dezember 2013 erstmals 5 Mio. Suchanfragen pro Tag

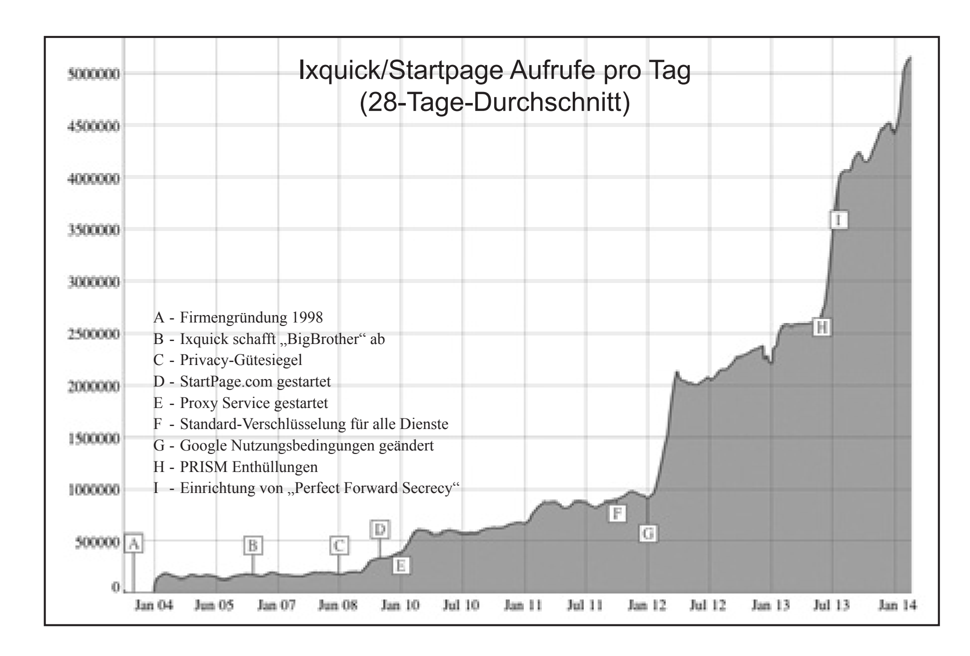
Am 23. Dezember 2013 überschritten die Suchanfragen auf den datenschutzfreundlichen Suchmaschinen startpage.com und ixquick.com erstmals die Grenze von 5 Millionen Suchanfragen am Tag. Anfang 2013 waren es noch 2,5 Millionen täglich. Im Laufe des Jahres 2013 wurden von Ixquick und StartPage insgesamt über 1,25 Milliarden Suchanfragen verarbeitet. „Jedes Mal, wenn Edward Snowden neue Details über die Spionageaktivitäten der US-Regierung enthüllt hat, konnten wir einen Ansturm neuer Nutzer verzeichnen“, erklärt Unternehmenssprecherin und Datenschutz-Expertin Dr. Katherine Albrecht. „Er hat versprochen, dass er 2014 noch mehr aufdecken will. Und soweit uns bekannt ist, hat er noch Material für mindestens zwei Jahre in der Hinterhand.“ Wie die Grafik von StartPage zeigt, sieht das Unternehmen die Gründe für die Steigerung seiner Nutzerzahlen vor allem in der Änderung der Datenschutzbestimmungen von Google und dem Bekanntwerden des PRISM-Skandals.

Die Nutzer seien verärgert darüber, dass bekannte Suchmaschinen sie ausspionieren würden, um persönliche Profile anzulegen und gezielt Werbung ausliefern zu können, so Albrecht. Und weiter: „Internet-Nutzer sind zurecht empört, dass die Regierungen diese Services belauschen und Zugang zu deren Datenbanken verlangen.“ StartPage rief anlässlich des Europäischen Datenschutztags dazu auf, die Privatsphäre zu revolutionieren. Dazu bedürfe es nur fünf Schritten:

- Internetnutzer sollen ihre bisherige Suchmaschine durch die datenschutzfreundlichen Suchmaschinen Start Page.com oder Ixquick.com ersetzen.
- Eine dieser Suchmaschinen soll als Startseite eingerichtet werden.
- Die datenschutzfreundlichen Suchmaschinen sollen auch auf mobilen Endgeräten genutzt werden.
- Websitebetreiber sollen eine StartPage- oder Ixquick-Suchbox auf ihrer Website einrichten.
- User sollen die Internetsuche nicht mit „Google es“ sondern mit „StartPage es“ oder „Ixquicke es“ bezeichnen.

Ixquick und die Schwestersuchmaschine StartPage bilden zusammen die größte anonyme Suchmaschine der Welt. „Unsere Datenschutzrichtlinie ist sehr einfach“, erklärt die Unternehmenssprecherin. „Wir sammeln keine persönlichen Informationen unserer Besucher - nichts, gar nichts, null. Es werden weder IP-Adressen aufgezeichnet, noch Tracking-Cookies eingesetzt. Sollte je eine Regierung an unsere Tür klopfen, gibt es für sie nichts zu holen.“

Wie Statistiken der Marktanteile der größten Suchmaschinen zeigen, ist die Beliebtheit der Suchmaschine Google vor allem in Deutschland jedoch ungebrochen – trotz schlechten Datenschutzniveaus und Überwachungsskandal. Im Dezember 2012 hatte Google in Deutschland einen Marktanteil von 89,9 %. Darauf folgten Bing mit 2,2 % und T-Online mit 1,3 % (Ask 1,1 %, Yahoo 0,9 %, web.de 0,7 %, Sonstige 3,1 %).



Im Dezember 2013 lag der Marktanteil von Google schon bei 90,5 %. Den zweiten und dritten Platz belegten wieder Bing und T-Online mit 3,2 % und 1,1 % (Ask 0,7 %, Yahoo 1,6 %, Conduit 0,4 %, web.de 0,7 %, Sonstige 1,8 %). Auch international ist Google an der Spitze. Der Markanteil betrug im Dezember 2013 68,1 %. Im Dezember 2012 lag der Marktanteil sogar noch bei 83,42 %. Die prozentuale Verschlechterung liegt vor allem an der Verbesserung des Marktanteils der Suchmaschine Baidu, und zwar von 1,67 % in 2012 auf 18,84 % in 2013. Die Suchmaschine Baidu wird von dem gleichnamigen chinesischen Unternehmen betrieben. Baidu ist Marktführer in China und spielt hierzulande fast keine Rolle.

Auch die Anzahl an Suchanfragen auf Google zeigt die geballte Macht der Suchmaschine. Schätzungen zufolge verarbeitet Google 3 – 4 Milliarden Suchanfragen pro Tag. Es gibt also noch viel zu tun in der Revolution der Privatsphäre. (Snowden-Effekt: Internet-Nutzer kehren großen Suchmaschinen aus Angst vor Überwachung den Rücken, PE StartPage 15. Januar 2014; Europäischer Datenschutztag: Nutzen Sie noch immer eine Pre-Snowden Suchmaschine? PE StartPage www.startpage.com 27. Januar 2014; Suchmaschinen Martanteile: Statistik für Dezember 2012, www. Web-stats. info 31.12.2012; Suchmaschinen Marktanteile: Statistik für November 2013; Panagiotis Kolokythas, Dezember 2013 Aktuelle Markanteile – Browser, OS und Suchmaschinen, www.pcwelt. de 09.01.2014; Panagiotis Kolokythas, Dezember 2012 Aktuelle Marktanteile – Browser, OS und Suchmaschinen, www. pcwelt.de, 02.01.2013)

Rechtsprechung

BVerfG

Beobachtung von gemäßigtem Linken-Politiker verfassungswidrig

Das Bundesverfassungsgericht (BVerfG) hat sich in einem Beschluss vom 17.09.2013 zu den Voraussetzungen für die Beobachtung von Abgeordneten durch Behörden des Verfassungsschutzes geäußert (Az. 2 BvR 2436/10, 2 BvE 6/08). Diese Beobachtung ist nicht nur ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung, sondern zugleich ein Eingriff in das freie Mandat. Die langjährige Beobachtung des Beschwerdeführers Bodo Ramelow, ehemals Bundestags- und danach Landtagsabgeordneter für die Partei Die Linke in Thüringen und dort aktuell Fraktionsvorsitzender, genügte den strengen Verhältnismäßigkeitsanforderungen nicht.

Das Bundesamt für Verfassungsschutz (BfV) beobachtet einzelne Mitglieder des Deutschen Bundestags, die der Fraktion Die Linke angehören. Seit 1986 führte es über Ramelow eine Personenakte, in der Informationen gesammelt sind, die bis in die 1980er Jahre zurückreichen. Die gesammelten Informationen betreffen dessen Tätigkeit in der und für die Partei sowie ab 1999 auch seine Abgeordnetentätigkeit, jedoch ohne sein Abstimmungsverhalten und seine Äußerungen im Parlament sowie in den Ausschüssen. Das BfV wertete jedoch parlamentarische Drucksachen aus und gewann auch Informationen über sonstige politische Aktivitäten Ramelows. Nach den Feststellungen der Fachgerichte ist Ramelow individuell nicht verdächtig, Bestrebungen gegen die freiheitliche demokratische Grundordnung zu verfolgen. Seine Beobachtung wurde ausschließlich mit seiner Mitgliedschaft und seinen Funktionen in der Partei begründet.

Mit seiner Verfassungsbeschwerde wehrte sich Ramelow gegen ein seine Beobachtung billigendes Urteil des Bundesverwaltungsgerichts (BVerwG) vom 21.07.2010 (BVerwGE 137, 275). Wegen der Verletzung des freien Mandats hob das BVerfG dieses Urteil auf und verwies die Sache zurück an das BVerwG. Das freie Mandat gemäß Art. 38 Abs. 1 Satz 2 GG gewährleistet die

freie Willensbildung des Abgeordneten und damit auch eine von staatlicher Beeinflussung freie Kommunikationsbeziehung zwischen dem Abgeordneten und den WählerInnen. Das Gebot freier Willensbildung steht in engem Zusammenhang mit dem Grundsatz der parlamentarischen Demokratie gemäß Art. 20 Abs. 2 Satz 2 GG. In der repräsentativen Demokratie des Grundgesetzes vollziehen sich die Willensbildung des Volkes und die Willensbildung in den Staatsorganen in einer kontinuierlichen und vielfältigen Wechselwirkung. Dieser kommunikative Prozess, bei dem der Abgeordnete nicht nur Informationen weitergibt, sondern auch Informationen empfängt, wird durch das freie Mandat geschützt. Zu diesem Schutz gehört auch die Freiheit der Abgeordneten von exekutiver Beobachtung, Beaufsichtigung und Kontrolle. Zudem besteht ein enger Zusammenhang mit dem Grundsatz der Gewaltenteilung gemäß Art. 20 Abs. 2 Satz 2 GG. Die einzelnen Abgeordneten sind zwar nicht von vornherein jeder exekutiven Kontrolle entzogen. Diese ist jedoch in erster Linie eine eigene Angelegenheit des Deutschen Bundestages, der dabei im Rahmen der Parlamentsautonomie handelt.

Die Freiheit des Abgeordneten von exekutiver Beobachtung, Beaufsichtigung und Kontrolle gilt - vermittelt über Art. 28 Abs. 1 GG - auch für die Mitglieder der Volksvertretungen in den Ländern. Ein Überwiegen des Interesses am Schutz der freiheitlichen demokratischen Grundordnung (fdgO) kommt nach Ansicht des BVerfG in Betracht, wenn Anhaltspunkte dafür bestehen, dass der Abgeordnete sein Mandat zum Kampf gegen die fdgO missbraucht oder diese aktiv und aggressiv bekämpft. Dabei kann die Parteimitgliedschaft des Abgeordneten ein Aspekt der gebotenen Gesamtbeurteilung sein. Wegen der wichtigen Rolle der Parteien für die politische Willensbildung des Volkes ist aber grds. davon auszugehen, dass ein parteipolitisches Engagement, welches seinerseits auf dem Boden der fdgO steht, diese stärkt. Für sich genommen vermag die bloße Parteimitgliedschaft daher allenfalls eine vorübergehende Beobachtung zu rechtfertigen. Das Urteil des BVerwG trug diesen Maßstäben nicht hinreichend Rechnung. Dabei ging das BVerfG von der Feststellung der Fachgerichte aus, dass keine heimliche Informationsbeschaffung erfolgte. Nach Ansicht des BVerfGs sind Normen im Bundesverfassungsschutzgesetz (BVerfSchG) hinreichend bestimmt. Die Entscheidung, ob Mitglieder des Deutschen Bundestages durch das BfV beobachtet werden dürfen, hat der Gesetzgeber bejaht und dabei der besonderen Schutzwürdigkeit von Abgeordneten ausreichend Rechnung getragen, indem § 8 Abs. 5 BVerfSchG fordert, dass diese Beobachtung verhältnismäßig sein muss.

Das war sie nach Ansicht des zweiten Senats des BVerfGs im Fall von Ramelow nicht. Die Fachgerichte hatten ausdrücklich festgestellt, dass dieser individuell nicht verdächtig ist, verfassungsfeindliche Bestrebungen zu verfolgen. Tatsächliche Anhaltspunkte dafür gäbe es nur in Bezug auf einzelne Untergliederungen der Partei Die Linke, denen Ramelow nicht angehört. Von ihm geht daher, so das BVerfG, kein relevanter Beitrag für eine Gefährdung der fdgO aus. Im Übrigen könnte das Verhalten des Beschwerdeführers - insbesondere, ob er die radikalen Kräfte aktiv bekämpft - seine Beobachtung allenfalls dann rechtfertigen, wenn diesen Kräften bereits ein bestimmender Einfluss innerhalb der Partei zukäme, was nicht festgestellt wurde.

Das BVerwG hatt dem gegenüber angenommen, Ramelows Tätigkeit sei dennoch objektiv geeignet, die verfassungsfeindlichen Bestrebungen zu unterstützen; gefährlich für die fdgO könnten auch Personen sein, die selbst auf deren Boden stünden, jedoch bei objektiver Betrachtung durch ihre Tätigkeit verfassungsfeindliche Bestrebungen förderten, ohne dies zu erkennen oder als hinreichenden Grund anzusehen, einen aus anderen Beweggründen unterstützten Personenzusammenhang zu verlassen. Das BVerwG wurde außerdem gerügt, dass es die eingesetzten Mittel des BfV akzeptierte, soweit es das Verhalten im von Art. 46 Abs. 1 GG besonders geschützten parlamentarischen Bereich betraf. Bei der festgestellten Sammlung und Auswertung parlamentarischer Drucksachen hatte die insoweit erforderliche Abwägung nicht stattgefunden.

Die Linke feierte den Beschluss als vollen Erfolg. Der Fraktionschef im Bundestag Gregor Gysi meinte, es handele sich um „einen wichtigen Tag in unserer Geschichte" und einen Schritt zur Gleichstellung der Linken. Die Parteivorsitzende Katja Kipping ergänzte: „Das ist ein klares Signal dafür, dass generell die Beobachtung und Kriminalisierung der Linken eingestellt werden muss." Es waren zum Zeitpunkt der Entscheidung des BVerfGs noch etwa 50 teilweise vergleichbare Fälle anhängig (BVerfG PE v. 09.10.2013; Janisch/Brössler, Erfolg für Linkspartei in Karlsruhe, SZ 17.10.2013, 1).

BVerwG

Keine pauschale Auskunftsverweigerung

Im Sommer 2006 hatte das Magazin Der Spiegel enthüllt, dass die politische Arbeit des Berliner Sozialforums systematisch durch Spitzel des Landes- und des Bundesverfassungsschutzes ausgespäht wurde. Alle darauf gestellten Anträge auf Akteneinsicht wurden pauschal mit dem Hinweis auf Quellenschutz abgelehnt. Mehrere Mitglieder des Sozialforums klagten deshalb gegen das Land Berlin. Das Verwaltungsgericht (VG) Berlin wies 2008 den Berliner Verfassungsschutz auf die Grenzen des Auskunftsverweigerungsrechts hin. Der zuständige Richter argumentierte, eine Auskunft über gespeicherte und gesammelte Informationen dürfe nicht pauschal verweigert werden. Nicht alle mit nachrichtendienstlichen Mitteln gewonnenen Informationen würden grundsätzlich Geheimnisschutz genießen, so wie der Verfassungsschutz argumentierte. Das sahen die Richter des Oberverwaltungsgerichts (OVG) 2010 in zweiter Instanz allerdings anders und hoben die Entscheidung des VG auf. Mit Urteil vom 02.11.2013 hob nun das Bundesverwaltungsgericht (BVerwG) das Urteil des OVG auf. In einem nächsten Schritt muss sich das OVG Berlin noch einmal mit dem Antrag auf Akteneinsicht und Auskunft befassen (Langes Nachspiel des Spitzeleinsatzes im Berliner Sozialforum, www.scharf-links.de 02.11.2013).

BGH

Keine Detailauskunft über Score-Berechnung

Gemäß einer Entscheidung des Bundesgerichtshofes (BGH) in Karlsruhe vom 28.01.2014 auf die Revision einer 54-jährigen Angestellten hin muss die Schufa Verbrauchern nicht erklären, wie sie zu den Werten für ihre Kreditwürdigkeit (Scores) gekommen ist (Az. VI ZR 156/13). Das Landgericht Gießen hatte im März 2013 als Berufungsinstanz entschieden, dass die bisherige Auskunftspraxis der Schufa den Anforderungen des Bundesdatenschutzgesetzes genügt. Das Unternehmen gibt auf Anfrage Auskunft über die gespeicherten Daten, nicht aber über seine Rechenmethode. Derartige Schufa-Auskünfte werden jährlich rund 680 000 Mal angefordert. Die Bewertungen der Schufa und anderer Auskunfteien sind für Millionen Menschen wichtig, die bei Krediten oder Mietverträgen auf eine positive Auskunft angewiesen sind.

In der Verhandlung kritisierte der Anwalt der Klägerin, Wendt Nassall, die Wirtschaftsauskunftei in Wiesbaden habe nur eine allgemeine Auskunft zur Kreditwürdigkeit seiner Mandantin gegeben. Die Schufa müsse auch erklären, wie die als Scoring bezeichnete Bonitätsbewertung zustande gekommen sei. Es sei klar, dass es im Massengeschäft der Schufa nur nach „Schema F“ gehen könne. „Dieses Schema F muss aber auch transparent sein“, verlangte der Anwalt und verwies auf den 2010 eingeführten Paragrafen 34 im Bundesdatenschutzgesetz. Die Klägerin erklärte, es habe sie tief verletzt, dass sie aufgrund einer Verwechslung seitens der Schufa zunächst gar keine Finanzierung für ihren geplanten Autokauf bekommen habe: „Sie kommen sich da vor wie abgewertet.“ Der Irrtum war zwar aufgeklärt und der Kredit doch noch genehmigt worden. Dennoch wollte die Frau wissen, wie die Schufa zu ihrer Einschätzung gekommen war.

Als Vertreter der Schufa erklärte Anwalt Matthias Siegmann in der Verhandlung, die Formel für das Scoring sei Geschäftsgeheimnis des Unternehmens. Die vom Gesetz geforderte Auskunft sei der Klägerin gegeben worden. Die Branche hatte das Urteil mit Spannung erwartet. Daten- und Verbraucherschützer hatten - vergeblich - gehofft, dass der Grundsatz der Transparenz in den vergangenen Jahren auch für den BGH in der rechtlichen Bewertung an Gewicht gewonnen habe. Christian Gollner von der Verbraucherzentrale Rheinland-Pfalz forderte umfassende Informationen für die Verbraucher: „Nur so können sie erfahren, wie sie eine schlechte Bewertung korrigieren und wie sie ihren Bonitätswert in Zukunft positiv beeinflussen können.“

Nach Ansicht des BGH hat die Schufa Auskunft darüber zu erteilen, welche personenbezogenen, insbesondere kreditrelevanten Daten bei ihr gespeichert und in die Berechnung der Wahrscheinlichkeitswerte eingeflossen sind. Diese Auskunft hat die Beklagte gegenüber der Klägerin (teilweise erst im vorliegenden Verfahren) erteilt. Ihr wurden alle bei der Beklagten zu ihrer Person gespeicherten Daten übermittelt. Ferner wurde sie über die in den letzten zwölf Monaten an Dritte übermittelten und die aktuell berechneten Wahrscheinlichkeitswerte sowie über die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten informiert. Die Einzelheiten wurden in einem Merkblatt erläutert.

Ein darüber hinausgehender Auskunftsanspruch bestehe aber nicht. Die von der Klägerin beanspruchten konkreten Angaben zu Vergleichsgruppen zählten nicht zu den Elementen des Scoringverfahrens, über die nach § 34 Abs. 4 Satz 1 Nr. 4 BDSG Auskunft zu erteilen ist. Gleiches gelte für die Gewichtung der in den Scorewert eingeflossenen Merkmale. Dem Auskunftsanspruch des § 34 Abs. 4 BDSG liege die gesetzgeberische Intention zugrunde, trotz der Schaffung einer größeren Transparenz bei Scoringverfahren Geschäftsgeheimnisse der Auskunfteien, namentlich die sog. Scoreformel, zu schützen. Die Auskunftsverpflichtung solle dazu dienen, dass der Betroffene den in die Bewertung eingeflossenen Lebenssachverhalt erkennen und darauf reagieren kann. Hierzu bedürfe es keiner Angaben zu Vergleichsgruppen und zur Gewichtung einzelner Elemente. Das gesetzgeberische Ziel eines transparenten Verfahrens werde dadurch erreicht, dass für den Betroffenen ersichtlich ist, welche konkreten Umstände als Berechnungsgrundlage in die Ermittlung des Wahrscheinlichkeitswerts eingeflossen sind (Bundesgerichtshof entscheidet über Umfang einer von der Schufa zu erteilenden Auskunft, juris.bundesgerichtshof.de 28.01.2014; Kein Rechtsanspruch auf volle Transparenz bei der Schufa, www.focus.de 28.01.2014).

KG Berlin

Facebook-Freundefinder war unzulässig

Das Kammergericht Berlin (KG) bestätigte in zweiter Instanz mit Urteil vom 24.01.2014, dass Facebook in mehreren Punkten gegen deutsches Recht verstößt beziehungsweise verstoßen hat (Az. 5 U 42/12). Das Urteil geht auf eine Klage des Verbraucherzentrale Bundesverbandes (vzbv) aus dem Jahre 2010 zurück. Die Verbraucherschützer hatten den „Freundefinder“ in der damaligen Version sowie einige Vertragsbedingungen kritisiert. Sie waren zu dem Ergebnis gekommen, dass die Facebook Ireland Limited als Betreiberin der Plattform in mehreren Punkten gegen deutsches Recht verstößt. Dies hatte 2012 das Landgericht (Az. 16 O 551/10) entschieden und wurde nun vom KG als Berufungsinstanz bestätigt.

Am Freundefinder beanstandeten die Gerichte, dass Kontaktanfragen per Mail ohne Einwilligung der kontaktierten Person erfolgt waren. Facebook-Nutzende seien bei der Erstregistrierung nur unzureichend darauf hingewiesen worden, dass der Freundefinder ihr gesamtes E-Mail-Adressbuch importiere. Außerdem räume sich Facebook in den Allgemeinen Geschäftsbedingungen (AGB) widerrechtlich das umfassende Recht an der Nutzung von Inhalten seiner Mitglieder ein. Außerdem sei rechtswidrig, dass den Nutzenden nichts anderes übrig bleibt, als der Verarbeitung ihrer Daten zu Werbezwecken zuzustimmen. Das KG hat keine Revision zum Bundesgerichtshof zugelassen. Facebook müsste zwecks weiterer Überprüfung des Urteils zunächst Beschwerde gegen diese Nichtzulassung einlegen.

Der vzbv ließ offen, wie er auf das Kammergerichtsurteil reagieren wird, so Carola Elbrecht: „Gegenüber 2010 haben sich bei Facebook einige von uns monierten Dinge geändert. Wir müssen

jetzt prüfen, ob die Plattform noch gegen einzelne Punkte im Urteil verstößt." Zumindest der Freundefinder habe sich so geändert, dass das Urteil wohl eher keine Anwendung mehr finde. Genau hinsehen wolle man insbesondere bei der beanstandeten Änderungsklausel zu den Datenschutzbestimmungen, die den Informationspflichten der Plattform gegenüber den Kunden nicht Genüge tat. Bei Facebook müsse man ständig am Ball bleiben, weil sich die Plattform ständig ändere: „Nun haben wir ein Loch geschlossen, aber es tut sich sicherlich ein neues auf" („Freundefinder": Facebook unterliegt Verbraucherschützern in zweiter Instanz, www.heise.de 27.01.2014).

VG Hannover

Personalausweisdaten dürfen nicht abgespeichert werden

Das Verwaltungsgericht (VG) Hannover hat es einem Automobil-Logistikunternehmen mit Urteil vom 28.11.2013 untersagt, zur Überwachung des Speditionsvorgangs die Personalausweise der Fahrzeugabholer einzuscannen und abzuspeichern (Az. 10 A 5342/11). Nach dem eindeutigen Willen des Gesetzgebers ist das unbeschränkte Erfassen der Daten - und damit auch das Einscannen und Speichern durch ein Unternehmen - untersagt.

Die klagende Logistikdienstleisterin aus Rehden, die insbesondere in der Automobillogistik tätig ist - lagert auf ihrem Betriebsgelände ständig mehrere tausend Kraftfahrzeuge. Täglich wird eine Vielzahl von Fahrzeugen abgeholt, die den Abholenden - insbesondere Fahrern von Speditionen - übergeben werden. Um den Speditionsvorgang zu überwachen, werden die Personalausweise der Abholenden eingescannt und auf einem eigenen Rechner gespeichert. Der Landesbeauftragte für den Datenschutz (LfD) Niedersachsen hatte der Klägerin aufgegeben, das Einscannen von Personalausweisen zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen.

Das VG Hannover hat die Klage gegen die Untersagung des Speicherns und die Anordnung des Löschens abgewiesen, weil diese rechtmäßig seien. Nach den hier anzuwendenden Vorschriften des Personalausweisgesetzes sei der Personalausweis ein Identifizierungsmittel, das der Inhaber vorlege und vorzeige, um sich auszuweisen. Nach dem eindeutigen Willen des Gesetzgebers sei aber das unbeschränkte Erfassen der Daten - und damit auch das Einscannen und Speichern durch ein Unternehmen - untersagt. Dadurch solle die Datensicherheit geschützt werden, weil einmal erfasste und gespeicherte Daten leicht missbräuchlich verwendet werden könnten. Das Gericht hat nicht den Vorwurf gegen die Klägerin erhoben, sie verwende die Daten missbräuchlich. Um den Zweck des Gesetzes zu erfüllten, dürften aber so wenig Daten wie möglich in Umlauf gebracht werden, so dass auch die Praxis der Klägerin zu untersagen sei (Gericht: Personalausweise dürfen nicht eingescannt und gespeichert werden, www.heise.de 29.11.2013; Einscannen und Speichern von Personalausweisen unzulässig, www.verwaltungsgericht-hannover.niedersachsen.de 28.11.2013).

LG Berlin

Google-Klauseln rechtswidrig

Das Landgericht (LG) Berlin hat in einem - nicht rechtskräftigen - Urteil vom 19.11.2013 nach einer Klage des Verbraucherzentrale Bundesverbands (vzbv) zahlreiche Vertragsklauseln des Internetkonzerns Google für rechtswidrig erklärt (Az. 15 O 402/12). Betroffen sind insgesamt 25 Klauseln aus den Nutzungs- und Datenschutzbestimmungen, die zu unbestimmt formuliert waren oder die Rechte der VerbraucherInnen unzulässig einschränkten.

Google hatte sich in der Datenschutzerklärung unter anderem das Recht vorbehalten, „möglicherweise" gerätespezifische Informationen und Standortdaten zu erfassen oder „unter Umständen" personenbezogene Daten aus den verschiedenen Google-Diensten miteinander zu verknüpfen. Für VerbraucherInnen bleibt so unklar, wozu sie ihre Zustimmung genau erteilen sollten. Zudem konnten personenbezogene Daten auch ohne aktive Einwilligung erfasst, ausgewertet und weiterverarbeitet werden. Aus Sicht des vzbv ist eine rechtskonforme Einwilligung in die Nutzung personenbezogener Daten nicht möglich, indem VerbraucherInnen bei der Registrierung lediglich die Erklärung ankreuzen: „Ich stimme den Nutzungsbedingungen von Google zu und habe die Datenschutzerklärung gelesen."

Zwölf Nutzungsbedingungen enthielten Formulierungen, die die Rechte der Verbraucher einschränkten. Der Konzern behielt sich auch vor, sämtliche in den Diensten eingestellte Daten zu überprüfen, zu ändern und zu löschen, Anwendungen sogar durch direkten Zugriff auf das Gerät zu entfernen sowie Funktionen und Features der Dienste nach Belieben komplett einzustellen. Nur sofern es „vernünftigerweise möglich" sei, werde die NutzerIn vorab über die Änderung des Dienstes informiert. Eine Erläuterung, was darunter zu verstehen ist, fehlte. Zudem nahm sich Google das Recht, die Nutzungsbestimmungen einseitig ohne Einwilligung der VerbraucherIn zu ändern. Der vzbv hielt das für unangemessen benachteiligend. Das LG schloss sich im Ergebnis dieser Auffassung an und erklärte die eingeklagten Bedingungen für rechtswidrig.

Gerd Billen, Vorstand des vzbv: „Das Urteil ist ein wichtiges Signal an die IT-Unternehmen. Sie müssen in Sachen Datenschutz umdenken und deutsche Datenschutzbestimmungen und Verbraucherschutzvorschriften ernstnehmen." Seit Jahren geht der vzbv gegen unwirksame Datenverarbeitungsklauseln vor. Das ist allerdings nur möglich, wenn die Datenschutzbestimmungen als Teil der Allgemeinen Geschäftsbedingungen (AGBs) gewertet werden. Andernfalls fehlt den Verbraucherzentralen nach geltendem Recht ein Klageinstrument, um unzulässige Praktiken zu unterbinden, zum Beispiel wenn zu Unrecht Daten von Verbrauchern erhoben oder weitergegeben werden. Deshalb fordert Billen: „Verbraucherverbände müssen ohne Hürden auch gegen datenschutzrechtliche Verstöße vorgehen können. Wir brauchen dringend eine erweiterte Klagebefugnis." Die neue Bundesregierung müsse eine entsprechende Regelung schaffen.

Google will in Berufung gehen, so ein Sprecher: „Wir sind davon überzeugt, dass unsere Nutzungsbedingungen und unsere Datenschutzerklärung im Einklang mit den entsprechenden Gesetzen sind.“ Der Konzern kritisiert, die Verbraucherschützer seien nicht befugt, gegen die Datenschutzerklärung des Konzerns zu klagen, weil diese nicht Teil der Allgemeinen Geschäftsbedingungen seien. Sollte Google auch in den weiteren Instanzen unterliegen und bei der jetzigen Praxis bleiben, droht ein Ordnungsgeld, das aber im Vergleich zum Umsatz des Konzerns gering ausfallen dürfte. Die vzbv-Juristin Bianca Skutnik meint aber: „Irgendwann wird es weh tun“ (Romberg, Druck auf Google, SZ 21.11.2013, 37; PE vzbv v. 19.11.2013, vzbv gewinnt Klage gegen Google, www.vzbv.de/12512.htm).

LG Hamburg

Max Mosley gewinnt in Europa den zweiten Prozess gegen Google

Am 24.01.2014 hat das Hamburger Landgericht (LG) das Urteil im Zivilprozess des Ex-Motorsportboss Max Mosley gegen Google gesprochen (Az. 324 O 264/11). Google darf sechs heimlich aufgenommene Sex-Bilder von Max Mosley nicht weiter verbreiten. Die Fotos aus dem Video einer privaten Party mit Prostituierten darf Google in den Suchergebnissen auf Google.de nicht mehr anzeigen. Nach Ansicht des Gerichts verletzt die Veröffentlichung der Bilder den 73-Jährigen schwer in seiner Intimsphäre. Sollte Google gegen die Auflage verstoßen, droht ein Ordnungsgeld von bis zu 250.000 Euro.

Die Pressekammer äußerte sich nicht dazu, wie Google das Urteil technisch umsetzen soll. Bei früheren Verhandlungsterminen hatte die Richterin jedoch eine Filtersoftware ins Spiel gebracht. Google kritisierte, dass aus der Suchmaschine eine „Zensurmaschine“ werden könnte. Das Urteil ist noch nicht rechtskräftig. Es ist Berufung beim OLG Hamburg möglich. Solange noch keine Rechtskraft eingetreten ist, muss Google die Fotos nicht zensieren.

Google-Anwalt Jörg Wimmers hatte nach der vorigen Verhandlung im September geäußert, die Forderung einer Filtersoftware werde zu einem „ziemlichen Beben im Unternehmen führen“. Der Konzern habe keine Technologie, die Kopien verbotener Bilder aufspüren und sperren kann. Da IT-Systeme zudem nicht fehlerfrei arbeiten, werde es immer Seiten geben, die trotz Rechtsverletzungen angezeigt werden und andersherum auch Seiten blockiert, die nicht gesperrt werden sollten. Nach Ansicht von Google werden durch die Zensur Grundrechte auf Informationsfreiheit aber auch Googles unternehmerische Freiheit eingeschränkt. Bei Google wird bislang nur Kinderpornographie – nach einer Vorprüfung durch das Bundeskriminalamt - herausgefiltert.

Mosley-Anwältin Tanja Irion widersprach dem Zensurvorwurf: „Herr Mosley würde sich freuen, wenn dieses Urteil auch anderen dabei hilft, den großen und nachhaltigen Schaden einzuschränken, der dadurch entsteht, dass Suchmaschinen Zugriff auf rechtswidrige Aufnahmen vermitteln.“

Mosley hat Google auch in Frankreich verklagt. In Paris erzielte Mosley im November einen Erfolg: Das Zivilgericht entschied, dass der US-Konzern neun Aufnahmen, die aus dem Video stammen, herausfiltern und sperren muss. In Frankreich drohen Google pro registrierten Rechtsverstoß 1000 Euro Strafe. Google geht gegen die Entscheidung des Gerichts bereits vor.

(Mosley gegen Google: Gericht entscheidet über Sex-Fotos, www.abendblatt.de 21.01.2014; Google darf Sex-Fotos von Max Mosley nicht anzeigen www.welt.de 24.01.2014; Urteil in Hamburg: Google darf Mosleys Sexfotos nicht verbreiten www.spiegel.de 24.01.2014)

LG Detmold

Kein vorbeugender Unterlassungsanspruch wegen Street View

Das Landgericht (LG) Detmold hat mit Urteil vom 12.10.2013 entschieden, dass einer Klage auf Unterlassung von Fotoaufnahmen durch Google Street View das Rechtsschutzbedürfnis fehlt, wenn die Aufnahmen noch nicht angefertigt wurden und der Betroffene vorab gegenüber dem Anbieter widersprochen hat (Az.: 12 O 153/10). Das Gericht stützt sich u.a. darauf, dass Google sich mit den deutschen Datenschutzbehörden auf eine Widerspruchsmöglichkeit für Betroffene verständigt hat. Im Fall des Widerspruchs des Berechtigten darf das betreffende Objekt danach nicht veröffentlicht werden, bzw. muss unkenntlich gemacht werden. Das schützt den Kläger nach Ansicht des Gerichts ausreichend, nachdem auch nicht ersichtlich ist, dass Google gegen diese Vereinbarung verstoßen würde. Mit der materiell-rechtlichen Frage, ob überhaupt ein Anspruch auf Unterlassung bestehen kann, der eine Verletzung des Persönlichkeitsrechts des Betroffenen oder datenschutzrechtlicher Vorschriften voraussetzen würde, setzte sich das Landgericht nicht auseinander (http://openjur.de/u/644431.html; Stadler, Kein vorbeugender Unterlassungsanspruch gegen Google Street View, http://www.internet-law.de 05.11.2013).

Buchbesprechungen



Sreball, Günther/Schmidt,
Stefan/Hermonies, Felix
Handbuch Datenschutz im Sport –
Formulare, Erläuterungen, Gesetze
Nomos Baden-Baden, 2014, 186 S.,
ISBN 978-3-8329-6887-8

(TW) Die Ausdifferenzierung des Datenschutzes nimmt ihren Lauf, so auch in der Praktikerliteratur. Dass der Schutz des Rechts auf informationelle Selbstbestimmung im Bereich des Sportes relevant ist, ist seit langem klar. Nun aber liegt erstmals zu diesem Thema ein Praxishandbuch vor. Dieses adressiert ehren- und hauptamtlich Aktive in Vereinen und Verbänden sowie Beratende, aber leider nicht die Betroffenen (SportlerInnen und andere, z. B Journalisten, Trainer, Familienangehörige). Mit kurzen einführenden Texten und ausgefeilten Hilfen und Formularen werden die meisten relevanten Sachverhalte, die typischerweise im Sportdatenschutz auftauchen, abgehandelt: Datenschutzbeauftragte, Verpflichtungserklärung für Mitarbeitende, Verfahrensverzeichnis, Vorabkontrolle, Auftragsdatenverarbeitung, Aufsichtsbehördentätigkeit, Satzungsregelungen, Mitgliedschaft, Werbung, Mitgliederverwaltung, Videobeobachtung. Daneben werden auch aktuelle neue und brisante Fragestellungen thematisiert: Webseiten, soziale Netzwerke, Dopingbekämpfung, Zuverlässigkeitsüberprüfung bei Großveranstaltung. Im Anhang finden sich die einschlägigen Gesetze abgedruckt, allen voran das Bundesdatenschutzgesetz.

Die Themen sind durch ein übersichtliches Inhaltsverzeichnis und durch ein etwas kurz geratenes und deshalb unvollständiges Stichwortverzeichnis erschlossen. Ergänzt wird die Text durch einige zumeist erläuternden Fußnoten, die teilweise auf weitere Quellen verweisen. Der Charakter des Praktikerhandbuchs wird dabei aber nicht verlassen, so dass einschlägige Dissertationen oder bestehende wissenschaftliche Veröffentlichungen nicht berücksichtigt sind. Hier liegt auch die Schwäche des Buches: es lässt sich praktisch nicht auf kontroverse Diskussionen zum Sportdatenschutz ein, von denen es viele gibt. So wird die hochheikle, massiv umstrittene und aus Sicht des Rezensenten verfassungswidrige Dopingbekämpfungspraxis unvollständig und eher affirmativ abgearbeitet. Ähnliches gilt etwa für die Akkreditierung von Großveranstaltungen, die von Datenschutzbeauftragten äußerst kritisch gesehen wird. Dabei wird weder auf landesspezifische Spezialregelungen eingegangen noch auf die besondere verfassungsrechtliche Problematik der Akkreditierung von JournalistInnen unter Einbeziehung von Polizei und Geheimdiensten. Die Autoren hätten sich nicht scheuen müssen, hier die bestehenden Kontroversen darzustellen und Position zu beziehen. Dies hätte die Lesenden nicht zwangsläufig irritiert, sondern eher die Intention des informationellen Grundrechtsschutzes erläutert und herausgehoben. Die ausschließlich auf formale Normerfüllung ausgerichtete Darstellung führt dazu, dass die Sicht der Betroffenen, etwa im Hinblick auf die Umsetzung ihrer Rechte, zu kurz kommt.

Es wird zwar dargestellt, wie dem bestehenden gesetzlichen Auftrag genügt werden kann; die ursprüngliche individualrechtliche wie gesellschaftliche Intention des Schutzes informationeller Selbstbestimmung gerät dabei leicht aus dem Blickfeld. Damit fördert das Buch die Position, Sport sei etwas Unpolitisches, das losgelöst von sonstigen gesellschaftlichen Realitäten praktiziert werden kann. Dessen ungeachtet sind die vorgelegten Formulare, Hilfen und Formulierungsvorschläge von einem hohen praktischen Nutzen. Wer sich den Grenzen des Buches bewusst ist, findet hier eine Vielzahl von Hilfen und Anregungen.



Härting, Niko
PinG Privacy in Germany - Datenschutz und Compliance
Erich Schmidt Verlag Berlin
ISSN: 2197-1862
1. Jahrgang, September 2013, S. 1-44
Einzelheft 25 €; Jahresabonnement 138 € (6x jährlich inkl. eJournal und Archiv)

Ein neues Fachjournal

(JR) Die Fachzeitschrift PinG erscheint seit September 2013. Herausgeber ist Prof. Niko Härting, Gründungspartner der renommierten Kanzlei HÄRTING Rechtsanwälte in Berlin und Autor des Fachbuchs „Internetrecht", welches mittlerweile in der 5. Auflage erschienen ist. Der PinG-Redaktion geht es um ein „zukunftsfähiges Datenschutzrecht und die unterschiedlichen Facetten der Informationsverarbeitung". Es sollen sowohl Datenschutz-Praktiker als auch Wissenschaftler angesprochen werden.

Redaktion und ständige Autoren der PinG sind – überwiegend erstaunlich junge – Juristen, die allesamt Datenschutzerfahrung gesammelt haben. Hauptsächlich handelt es sich um ehemalige Unternehmensjuristen. Unter den ständigen Autoren ist auch der Leiter der Stiftung Datenschutz, Frederick Richter. Darüber hinaus werden Artikel von Gastschreibern veröffentlicht. Die Redaktion will ein breites Meinungsspektrum bieten. Daher ist es von ihr ausdrücklich erwünscht, auch abseits der herrschenden Meinung zu diskutieren. Um den Praxisbezug herzustellen, lässt die Redaktion Datenschutz-Praktiker zu Wort kommen. Das Heft hat einen internationalen Anspruch und veröffentlicht daher auch englischsprachige Artikel.

Das Format soll außerdem intermedial sein. Daher bietet die Redaktion zusätzlich zum Fachjournal ein eJournal, einen Blog sowie einen Twitter- und YouTube-Kanal.

Das Heft im Detail

Jede Ausgabe besteht aus drei Rubriken: Privacy Topics, Privacy Compliance und Privacy News. In der Rubrik „Privacy Topics" werden unterschiedliche Themen rechtswissenschaftlich aufbereitet. In der ersten Ausgabe veröffentlichte die Redaktion einen Aufsatz von Prof. Dr. Hans Peter Bull (erster Bundesbeauftragter für den Datenschutz, 1978 – 1981) zur Neuordnung der Aufgaben und Befugnisse der Sicherheitsbehörden. Außerdem kommt in dieser Rubrik Dr. Kai von Lewinski (Rechtsanwalt bei Lovells mit Schwerpunkt Informations- und Datenschutzrecht) zu Wort, der in seinem Aufsatz Gründe für die Durchsetzungsmängel des Datenschutzes analysiert.

Die Rubrik „Privacy News" enthält kurze Diskussionsbeiträge zu aktuellen Themen. Es handelt sich zwar nicht um journalistische News, die Texte sind aber immerhin allgemeinverständlich. Insbesondere für den Nicht-Juristen sind diese Texte daher in Bezug auf den Lesefluss eine willkommene Abwechslung. In der ersten Ausgabe wirft Peter Schaar einen Blick zurück auf die letzten zehn Jahre als Bundesdatenschutzbeauftragter. Außerdem fordert der Geschäftsführer des Online-Unternehmens nugg.ad, Stephan Noller, eine Algorithmen-Ethik. Weitere Beiträge u. a. zur EU-Datenschutz-Grundverordnung und zum NSA-Skandal sowie ausgewählte Gerichtsverfahren und Rechtsprechung runden die zweite Rubrik ab.

In der Kategorie „Privacy Compliance" schreiben Datenschutz-Praktiker über den Datenschutz in Unternehmen. In der ersten Ausgabe sind drei Artikel veröffentlicht, und zwar zu Prüfungen der Datenschutz-Aufsichtsbehörden, datenschutzkonformen Mitarbeiterbefragungen und Outsourcing im Gesundheitswesen. Der Artikel zu Prüfungen der Datenschutz-Aufsichtsbehörden ist allgemein gehalten und bietet auf diese Weise wohl nur für den Datenschutz-Neuling wirklich Neues. Die Autoren der beiden anderen Artikel behandeln spezielle Themen der Datenschutz-Praxis, die vermutlich nicht jeden Datenschutz-Praktiker ansprechen. Diese letzte Rubrik dürfte gerne etwas länger und thematisch breiter aufgestellt sein, um für diesen Leserkreis einen größeren Nutzen zu bieten.

Mit 25 € je Ausgabe befindet sich PinG im Vergleich zu den etablierten Datenschutz-Fachzeitschriften im mittleren Preisniveau.

Fazit

Beim ersten Durchblättern der Zeitschrift PinG drängt sich die Frage auf, ob es wirklich noch einer weiteren Datenschutz-Fachzeitschrift bedarf. Beim Lesen erweist sich die PinG jedoch als ein interessantes neues Format. Erfrischend sind vor allem die eher kurzen Artikel der Rubrik „Privacy News". Die rechtswissenschaftlichen Aufsätze ermöglichen einen Blick über den Tellerrand und liefern – hoffentlich bald mehr – Handlungsanreize für die Praxis. In der ersten Ausgabe ist es der Redaktion zudem gelungen, ein ausgewogenes Verhältnis der unterschiedlichen Auslegungen des Datenschutzrechts zu liefern. Diese erste Ausgabe ist gelungen und macht Lust auf die kommenden!

Cartoon





BvD-Datenschutztage 2014

Wettbewerbsfaktor Datenschutz

21. und 22. Mai 2014 in Berlin







- **Herausragende Keyspeaker, u.a.**
  Heiko Maas, Bundesminister der Justiz und für Verbraucherschutz
  Jan Philipp Albrecht, MdEP, Berichterstatter EU-DSGVO
  Andrea Voßhoff, Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
  Dr. Kim Nguyen, D-trust
- **2 Tage intensives Networking mit fachkundigen Teilnehmern, Referenten und Vertretern von Aufsichtsbehörden**
- **Sonderseminare zur Fortbildung**
- **BvD-Mitgliederversammlung**
- **Fundierte Workshops zu aktuellen Herausforderungen im Datenschutz**

Veranstaltungsort: NH Berlin Mitte, Leipzigerstr. 106-111, 10117 Berlin

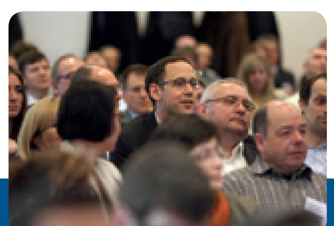
Wir haben im Tagungshotel NH-Berlin Mitte ein Kontingent an Zimmern für Sie reserviert: EZ 141,00 Euro incl. Frühstück, DZ 162,00 Euro incl. Frühstück Bitte buchen Sie direkt beim **NH-Berlin Mitte,** Stichwort „BvD-2014“

Anreise mit dem Zug
Nehmen Sie vom Hauptbahnhof die S5 in Richtung Straußberg oder die S7 in Richtung Ahrensfelde und steigen Sie an der Haltestelle Friedrichstraße aus. Steigen Sie in die U-Bahn U6 in Richtung Alt Mariendorf um und fahren Sie bis zur Haltestelle Stadtmitte. Das Hotel liegt auf der rechten Seite in der Leipziger Straße. Gesamtzeit: 10 bis 15 Minuten

Mit BvD und der Deutschen Bahn umweltfreundlich zur Tagung! Buchen Sie Ihr Deutsche Bahn Zugticket zu den Tagungen, Gruppentreffen und Fortbildungen des BvD. Preis/Person ab 99,00 €* hin und zurück. Buchungen unter: 01806 311153 (20 Cent/Minute, maximal 60 Cent pro Anruf aus den Mobilfunknetzen), Stichwort: BvD. *Weitere Infos unter www.bvdnet.de

Anreise mit dem Flugzeug
Von Tegel: Fahren Sie mit der Buslinie 128 bis zur U-Bahnstation Kurt-Schumacher-Platz. Steigen Sie in die U6 in Richtung Alt Mariendorf um. Fahren Sie bis zur Haltestelle Stadtmitte. Gesamtzeit: 25 Minuten.

Von Schönefeld: Nehmen Sie die S7 oder S14 in Richtung Hauptbahnhof. Steigen Sie an der Haltestelle Friedrichstraße aus und steigen Sie in die U-Bahnlinie U6 in Richtung Alt Mariendorf um. Steigen Sie an der Haltestelle Stadtmitte aus. Gesamtzeit: 40 Minuten







Anmeldung unter www.bvdnet.de